UNIVERSITI PUTRA MALAYSIA

ZERO DISTORTION-BASED STEGANOGRAPHY FOR HANDWRITTEN SIGNATURE

VAHAB IRANMANESH

FK 2018 78

ZERO DISTORTION-BASED STEGANOGRAPHY FOR HANDWRITTEN SIGNATURE

By

VAHAB IRANMANESH

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Doctor of Philosophy

January 2018

COPYRIGHT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Doctor of Philosophy

ZERO DISTORTION-BASED STEGANOGRAPHY FOR HANDWRITTEN SIGNATURE

By

VAHAB IRANMANESH

January 2018

Chairman : Associate Professor Sharifah Mumtazah Syed Ahmad, PhD
Faculty : Engineering

The growth of the Internet over the last few years has enabled many people and organisations, such as financial institutions, around the world communicate with each other and transfer information over public channels. In this light, public channels are used due the lack of private network infrastructure and high setup cost of private networks. However, the data would be transferred through several different networks before being delivered to the recipient and the information can be read or modified by unauthorized user(s). To overcome this problem, steganography can be utilised as a solution for privacy problems in public networks, such as the Internet, where many digital media, such as images, audio and texts exist.

Moreover, with the advancement of steganography, several researchers have recently devised steganalysis techniques, which threaten the steganographic systems. This means that any changes on the cover media (c) could lead to the identification of the stego media (s), which contains the secret message (m). Thus, developing a steganographic algorithm to use cover media (c) without raising attention is the most challenging task in data hiding. In this thesis, the human handwritten signature is introduced as a novel cover media (c) in conjunction with a steganography algorithm since there is a level of variability (i.e intra-user variability) within handwritten signature samples of an individual. To the best of our knowledge, this is the first time that a human handwritten signature sample is used for steganography application.

In its simplest form, the existence of intra-user variability within handwritten signature samples of an individual is explored using the Kruskal-Wallis hypothesis test. Next, hiding data was accomplished by implementing a signature synthesis technique to produce a synthetic signature sample as a stego signature (s). This step was conducted

by modelling both time series signals x and y (i.e. shape) of the handwritten signature samples using the maximum overlap discrete wavelet transform (MODWT) and several curve fitting techniques as the distortion function. Thus, the generated stego signature (s) is used to make stego key (k) based on the zero-distortion approach to represent the secret message (m) in a binary format. Finally, a computer numerical control (CNC) machine is utilized to plot the stego signature (s) on a piece of A4 paper for delivering to the recipient. On the other hand, by delivering the genuine signature sample as well as the stego key (k) using different channels such as the Internet, various image-processing techniques applied on the scanned stego signature (s) image to reconstruct the secret message (m).

It was found that the acceptable range for the intra-user variability for genuine signature samples in the SIGMA signature database can be shown as Mean ± 2STD for both time series signals x and y. In addition, the imperceptibility rates of 3.5% and 4.7% were obtained for machine learning and human perception evaluation approaches, respectively, when identifying the stego signatures (s). This study has also demonstrated the payload capacity rate as 45.17%, which was the average percentage of usage of the stego signature (s) for encoding the predefined secret message (m). Finally, the proposed technique was able to retrieve the hidden data using the selected offline stego signature sample ($\bar{s}$), with 94.7% accuracy rate.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

STEGANOGRAFI BERDASARKAN HEROTAN SIFAR UNTUK TANDATANGAN

Oleh

VAHAB IRANMANESH

Januari 2018

Pengerusi : Profesor Madya Sharifah Mumtazah Syed Ahmad, PhD
Fakulti : Kejuruteraan

Perkembangan Internet sejak beberapa tahun kebelakangan ini telah membolehkan sebilangan besar masyarakat dan pelbagai organisasi, seperti institusi kewangan, di seluruh dunia berkomunikasi antara satu sama lain dan memindahkan maklumat melalui saluran awam. Dalam hal ini, saluran awam digunakan kerana kekurangan infrastruktur rangkaian persendirian dan kos penyediaan rangkaian peribadi yang tinggi. Walau bagaimanapun, data akan dipindahkan melalui beberapa rangkaian yang berbeza sebelum dihantar kepada penerima dan maklumat tersebut boleh dibaca atau diubahsuai oleh pengguna tanpa kebenaran. Untuk mengatasi masalah ini, steganografi boleh digunakan sebagai penyelesaian kepada masalah kerahsiaan di rangkaian awam, sebagai contoh, di Internet, yang mengandungi banyak media digital, seperti imej, audio dan teks.

Tambahan pula, dengan perkembangan steganografi, baru-baru ini sebilangan penyelidik telah merangka teknik steganalisis, yang mengancam sistem steganografi. Ini bermakna bahawa sebarang perubahan pada media penutup (c) boleh membawa kepada penemuan media stego (s) yang mengandungi mesej rahsia (m). Oleh itu, usaha membangunkan algoritma steganografi untuk menggunakan media penutup (c) tanpa menarik perhatian adalah tugas yang paling mencabar dalam penyembunyian data. Dalam tesis ini, tandatangan tulisan tangan manusia diperkenalkan sebagai media penutup (c) baharu, untuk digunakan dengan algoritma steganografi kerana terdapat suatu tahap kebolehubahan (iaitu kebolehubahan intra-pengguna) dalam sampel tandatangan tulisan tangan individu. Berdasarkan pengetahuan kami, ini merupakan kali pertama sampel tandatangan bertulis manusia digunakan untuk aplikasi steganografi.

Secara ringkas, kewujudan kebolehubahan intra-pengguna dalam sampel tandatangan bertulis seseorang individu dikaji menggunakan ujian hipotesis Kruskal-Wallis. Seterusnya, data tersembunyi dicapai dengan menggunakan teknik mensintesis tandatangan untuk menghasilkan sampel tandatangan sintetik sebagai tandatangan stego (s). Langkah ini dilakukan dengan menghasilkan model kedua-dua isyarat masa x dan y (iaitu, bentuk) daripada sampel tandatangan bertulis menggunakan jelmaan gelombang kecil diskret bertindih maksimum (maximum overlap discrete wavelet transform, MODWT) dan beberapa teknik penyesuaian lengkung sebagai fungsi herotan. Oleh itu, tandatangan stego (s) yang dihasilkan digunakan untuk menghasilkan kunci stego (k) berdasarkan pendekatan herotan sifar untuk mewakili mesej rahsia (m) dalam format perduaan. Akhir sekali, mesin kawalan berangka terkomputer (computerized numerical control, CNC) digunakan untuk menghasilkan tandatangan stego (s) di atas sekeping kertas A4 untuk dihantar kepada penerima. Sebaliknya, dengan menghantar sampel tandatangan tulen berserta kunci stego (k) menggunakan saluran yang berlainan, seperti Internet, pelbagai teknik pemprosesan imej boleh digunakan terhadap imej tandatangan stego (s) yang diimbas untuk membina semula mesej rahsia (m).

Didapati bahawa julat yang boleh diterima untuk kebolehubahan intra-pengguna untuk sampel tandatangan tulen dalam pangkalan data tandatangan SIGMA boleh ditunjukkan sebagai purata ± 2STD untuk kedua-dua isyarat siri masa x dan y. Di samping itu, kadar ketidakpercayaan sebanyak 3.5% dan 4.7%, masing-masing diperoleh untuk pendekatan pembelajaran mesin dan penilaian persepsi manusia apabila mengenal pasti tandatangan stego (s). Kajian ini turut menunjukkan kadar kapasiti muatan sebanyak 45.17% yang merupakan purata peratusan penggunaan tandatangan stego (s) untuk pengekodan mesej rahsia (m) yang ditetapkan. Akhir sekali, teknik yang dicadangkan ini mampu mengambil kembali data yang disembunyi dengan menggunakan sampel tandatangan stego luar talian ($\overline{s}$) yang dipilih dengan kadar ketepatan sebanyak 94.7%.

ACKNOWLEDGEMENTS

Firstly, I would like to express my sincere gratitude to my advisor Associate Prof. Dr. Sharifah Mumtazah Syed Ahmad for the continuous support of my PhD study and related research, for his patience, motivation, and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my PhD study.

Besides my advisor, I would like to thank the rest of my thesis committee: Assoc. Prof. Dr. Wan Azizun Wan Adnan, Assoc. Prof. Dr. Salman Yussof and Dr. Marsyita Hanafi for their insightful comments and encouragement, but also for the hard question which incented me to widen my research from various perspectives.

Last but not the least, I would like to thank my family: my parents and wife for supporting me spiritually throughout writing this thesis and my life in general.

I certify that a Thesis Examination Committee has met on 3 January 2018 to conduct the final examination of Vahab Iranmanesh on his thesis entitled "Zero Distortion-Based Steganography for Handwritten Signature" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

M. Iqbal bin Saripan, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abd. Rahman bin Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Fakhrul Zaman bin Rokhani, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Danilo Mandic, PhD
Professor
Imperial College London
United Kingdom
(External Examiner)

RUSLI HAJI ABDULLAH, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 30 July 2018

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Sharifah Mumtazah Syed Ahmad, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Wan Azizun Wan Adnan, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Marsyita Hanafi, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Salman Yussof, PhD
Associate Professor
College of Computer Science and Information Technology
Universiti Tenaga Nasional
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: _____ Date:_____

Name and Matric No.: Vahab Iranmanesh , GS32684

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Associate Professor Dr. Sharifah Mumtazah Syed Ahmad

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Wan Azizun Wan Adnan

Signature: _____
Name of Member of Supervisory Committee: Dr. Marsyita Hanafi

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Wan Azizun Wan Adnan

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background

Nowadays, due to the growing of computer and the Internet usages, communicating in a secure way is an important element between parties in the globe. Therefore, people use the same secure channel to exchange the secret information. However, in a situation whereby an individual is unable to gain access to the secure channel for any reason, the individual would use the public channel such as the Internet to transfer the secret information but the security is not at an acceptable level.

A man-in-the-middle attack is one of the methods that intruders use to intercept the communication between parties (X. Xiao et al., 2011). In this technique, a hacker place himself between sender and receiver to eavesdrop the information that is passing through the public channel, which can be misused later on by him. To overcome this problem, cryptography is introduced as a protection mechanism to scramble and make the secret message unreadable (encrypted) before sending the sensitive data over the public channel (Blahut, 2014). This can be done using a private-key (symmetric) as well as public key (asymmetric) methods (Menezes, Van Oorschot, & Vanstone, 1997). As a matter of fact, the cryptography methods can be vulnerable due to the fast growing of the computer capabilities, especially the processing and memory. Moreover, the obviousness of the cipher text (unreadable data) can be the main factor in order to implement the methods to disclosure the encrypted data in to plain text (readable data), which are called cryptanalysis techniques. For instance, the quantum computing, which can process huge amount of data in a short period of time, can be used as a very fast computing device to break the current encryption algorithms using brute force attack (Ashiq JA, 2015; Natalie Wolchover, 2015). Additionally, due to this fact that intercepting the information, which are used cryptography techniques by criminals through public channel would be a difficult task, several governments are prohibited or limited the usage of encryption techniques (Meng, Hang, Yang, Chen, & Zheng, 2009; Saha, Sharma, & Sharma, 2012; M. Shirali-Shahreza, 2007). This gives us to the need of data hiding, which is an alternative mechanism that is used to secure the secret information from unauthorized parties.

As a matter of fact, data hiding techniques are categorized into two main approaches, steganography and watermarking. The steganography is referred to hiding secret data using various digital media (Sarkar, 2010). During the last decade, several governments and countries, especially the United States (U.S) have started to acknowledge and emphasize the importance of research in steganography domain for securing their individuals, societies, industries and national security after 9-11 incident (Conway, 2003). In this case, some steganography algorithms have been proposed, which utilized digital media such as images, audios and texts as the carrier to hide and

transfer the hidden data through public channel (Al-Othmani, Manaf, Zeki, & Lumpur, n.d.; Bhattacharyya, Banerjee, & Sanyal, 2011; saroha & Singh, 2009). The reason to use digital media as a vehicle is due to frequent usage of these digital media on the Internet as well as high rate of redundant information within them (H. Wang & Wang, 2004), which can be a potential opportunity to hide the data. For example, as Figure 1.1 shows, manipulating the least significant bit (LSB) of the pixels within an image, which cannot have such a degradation on the image is one of the main steganography method in order to hide the data in image steganography.

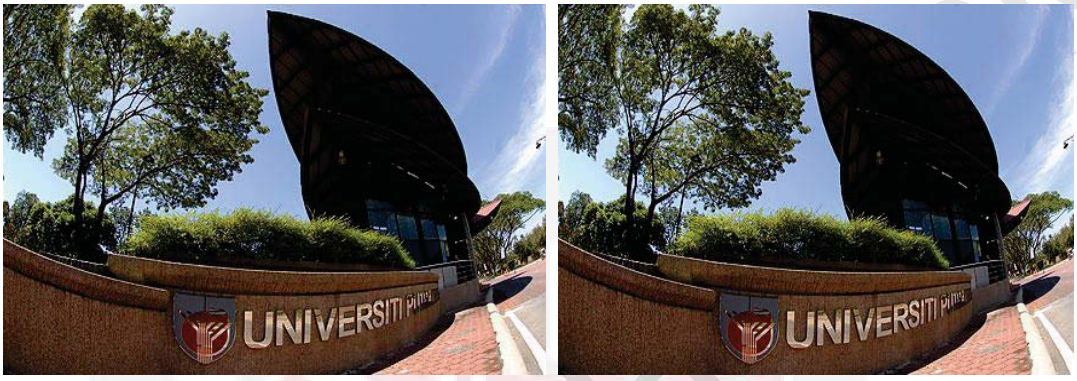

Figure 1.1 : Image Steganography Sample using LSB, Cover Image (left) and Stego Image (right)

Since the cryptography can conceal only the hidden data from the eavesdroppers, steganography can even hide the existence of the hidden data for additional security, which can also increase the confidentiality of the hidden data. Therefore, the hidden data cannot be detectable by unauthorized party on transmission through public channels, which is the main point of using steganography. Thus, this can decrease the level of suspicious by eavesdropper on the digital media that such as the image that contains the secret information. In contrast, watermarking is mostly used to verify the ownership of a digital media such as image by embedding the ownership message (watermark) into the digital media. Figure 1. 2 illustrates three main requirements which must be considered in each data hiding technique.

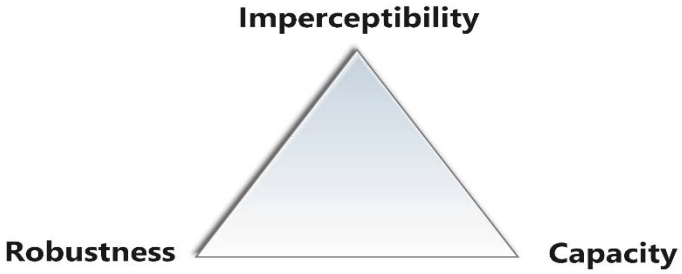

Figure 1.2 : Three Main Requirements of Data Hiding Technique

- Imperceptibility: which describes the un-detectability of stego media (*s*).
- Capacity: how much data/bits can be embedded in the cover media using a particular hiding method.
- Robustness: to extent to which, the decoder can retrieve the secret message while having noise or attack in the channel.

Since the main goal of steganography is to hide and transmit the hidden data over the public channel, the imperceptibility and capacity are two important attributes (Cetin & Ozcerit, 2009; Liang Zhang, Haili Wang, & Renbiao Wu, 2009; Salomon, 2003). In fact, there is no known method, which is widely used to evaluate the quality of each steganography algorithm. Thus, the imperceptibility as well as capacity are considered as two measures to evaluate the performance of the stenographic systems. Imperceptibility is referred to the degree of difference between both digital media, before and after carrying the secret information over public channel. In a case that this difference is very high and obvious, it can be used as an indicator for eavesdropper to identify the hidden communication. Thus, the high level of imperceptibility in stenographic system can prove the secrecy of the hidden communication and data. Furthermore, since the capacity is presented as the amount of data that the digital media can deliver to the recipient, there is an inverse relation between this measure and imperceptibility. It means that the more information will be hidden using digital media, the less imperceptibility will be occurred in the stenographic system. This is due to the high amount of distortion that is applied on the digital media for steganography purpose. On the other hand, robustness is the only important requirement against copyright violation in watermarking, since any illegal activity that would copy or modify the watermarked media. In other words, the concentration in steganography is on hidden data, which is considered as the secret message whereas the digital media is the main goal in watermarking.

As Figure 1.3 shows, each steganographic system includes two main parts, an encoding and decoding processes, which use the public channel to transmit the hidden data. The digital media that is used in the encoding phase for hiding data is called cover media (*c*). In addition, the hidden data that is concealed using the cover media (*c*) is referred to secret message (*m*) by using stego key (*k*). In fact, the stego key (*k*), which is an optional element, is used when the steganography algorithm is released to the public or known by attacker, therefore, like cryptography which is used key for encryption and decryption, the security of steganographic system can be relied on the stego key (*k*) (Simmons, 1984). Additionally, the sender is used the encoding function on the mentioned elements to hide the data. The output of the encoding function is called the stego media (*s*), which needs to be sent to the recipient side using the public channel to deliver the secret message (*m*). Similarly, the recipient will receive the same stego media (*s*) from the public channel, which requires decoding function, the reverse function of encoding, to reconstruct the hidden data, either using the same stego key (*k*) or not. In a case that the stenography algorithm is published to the public and attacker knows how the data can be hidden using the cover media, the stego key (*k*) can be the only part which without it, the intruder cannot reconstruct the hidden data

from the captured cover media (*c*). However, having a stego media (*s*) in a natural appearance is a chilling task since it must not attract the attention of eavesdropper.

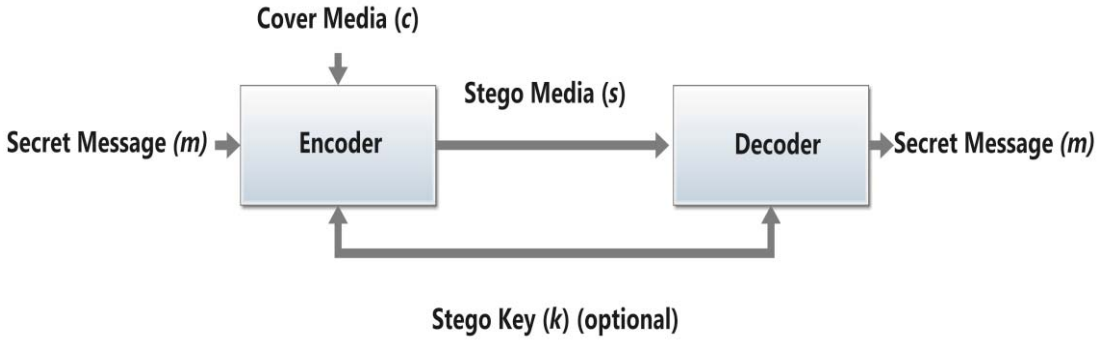

Figure 1.3 : Steganographic System

1.2 Problem Statement

With the advancement of steganography, several researchers have devised steganalysis techniques recently, which threaten the steganographic systems (Bhattacharyya et al., 2011; Chhikara & Singh, 2013; M. Kaur & Kaur, 2014). The main goal in steganalysis is to collect enough evidences in order to either detect the existence of secret message (*m*) or retrieve the hidden data within digital media such as image, audio and text (Nissar & Mir, 2010). In fact, steganalysis is based on known features, properties, media and steganography techniques that have already been investigated. Therefore, any changes on the cover media (*c*) can be led to identify the stego media (*s*). For example, in the image steganography domain, both steganography and steganalysis techniques are exploited the image pixels values, in spatial or frequency domains, since the pixels are the main elements to construct the image in order to embed or identify the secret message (*s*). Moreover, in a case that the properties and features of cover media (*c*) are not existed or complex to attain by the steganalys, and since the changes on the cover media (*c*) can effect on the statistical properties of cover media (*c*), the statistical analysis can be used to identify the stego media (*s*). To this end, the steganalysis can be considered as a pattern recognition problem, which is classified the digital media as either cover media (*c*) or stego media (*s*). In fact, if steganalyst could prove that somehow the cover media (*c*) is changed, which is referred to low imperceptibility, the steganography algorithm is considered unsuccessful. For instance, Figure 1.4 shows two histograms of the same image before (cover image) and after (stego image) embedding, which histogram analysis can be useful to represent this difference as the proper features for identifying the media (stego media) that contains the hidden data. Thus, developing a steganography algorithm to use cover media (*c*) without raising the attention of people is the most challenging task in data hiding.

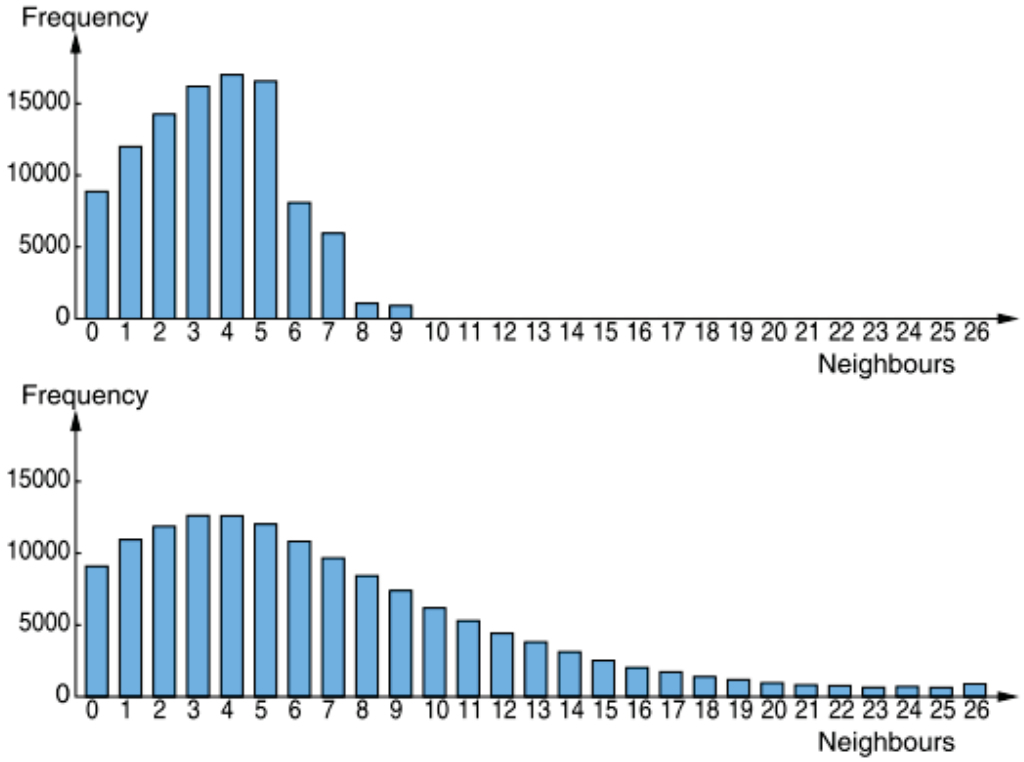

Figure 1.4 : Neighborhood Histogram, Cover Image (top) and Stego Image (bottom)
(Westfeld, 2003)

Nevertheless, more research on the steganography should be carried out to identify new potential cover media (*c*) which shows a degree of flexibility in conjunction with an appropriate steganography algorithm, which can have high imperceptibility as well as capacity for the steganography purpose, without drawing attention from steganalysis by manipulating limitation of human vision system. Thus, in this thesis, the human handwritten signature is introduced as a novel cover media (*c*) in conjunction with a steganography algorithm with high imperceptibility and capacity. As a matter of fact, the suggested cover media (*c*) is widely available, since the general public has been accustomed to writing down their signatures on the letters, cheques and documents as tokens for quick verification (Shafiei & Rabiee, 2003). This is mainly due to the ballistic nature of human signing operation, whereby human signature stabilized over a period of years, which eventually reflect ones identity. Nevertheless, human signatures do inherit some level of variability, which is called intra-user variability, among them (de Oliveira, A Kaestner, Bortolozzi, & Sabourin, 1997; Syed Ahmad, Shakil, Ahmad, Muhamad Balbed, & Anwar, 2008; Syed Ahmad, Shakil, Ahmad Faudzi, & Anwar, 2010). This low level of inconsistency is due to human's inability to reproduce the exact replicas of his signature samples on different times, which may be influenced by environmental, health and emotional challenges while signing (Impedovo & Pirlo, 2008; Kholmatov & Yanikoglu, 2005). However, such a small variability is acceptable, expected and as a matter of fact, an exact

signature replica is often suspected as forged sample (Mumtazah Syed Ahmad, Mohd Ali, & Azizun Wan Adnan, 2012; Syed Ahmad et al., 2010). For example, in a case that there is a lack of samples in a signature database for training as well as testing the signature biometric system, signature synthesis is used as a biometric synthesis technique to exploit the intra-user variability among the existing signature samples in order to generate artificial (synthetic) signature samples (Galbally, Plamondon, Fierrez, & Ortega-Garcia, 2012). In fact, several properties of original signature samples, which can take part to modify the structure of the signature (shape) slightly are used in order to generate the synthetic ones. Therefore, since the synthetic signature samples (fake) are similar to the original signature samples, they can be utilized as the original signature samples in signature biometric system. As a result, this study investigates the possibility of exploiting the intra-user variability within the signature samples for hiding the secret message (m) with high degree of imperceptibility and capacity.

1.3 Research Objectives

The main objective of this study is to investigate the possibility of using handwritten signature sample for steganography purpose, based on the zero-distortion approach. To achieve this aim, three objectives are constructed as follows:

1. To study the existence and acceptable range of intra-user variability of genuine human handwritten signature in SIGMA database.
2. To synthesise the human handwritten signature samples that contains a degree of variability.
3. To design and develop a signature steganography system using the synthesized signature samples developed in objective 2, based on the zero-distortion approach.
4. To evaluate the imperceptibility, payload capacity and data reconstruction accuracy of the developed steganography system.

1.4 Significance of the study

Current research work in steganography often emphasize on complex coloured images, audio and text media whereby all are mostly in digital formats. The established steganography techniques tend to manipulate limitation in human hearing and perception. Such algorithm may produce stego media (s) that appear to be conspicuous to human. However, they can be easily detected through the use of steganalysis techniques.

To the best of our knowledge, there has never been any attempt to hide the secret message (m) using human signatures, neither in digital format nor drawn on the paper. The ideas proposed in this study is novel. The objective is to use human signature by talking advantages of the intra-user variability that is inherent in signature samples,

thereby, providing for a new approach to steganography as well. Further, the proposed method is aimed at hiding the secret message (m) within an acceptable level of variability in human signature, with hope of eliminating detection, by both human and steganalysis techniques.

1.5 Research Scope

The scope of the research as follow:

1. The experimental dataset is limited to signature samples from SIGMA database
2. The intra-user variability within the genuine signature samples is used as the imperceptibility measure.
3. Using computer numerical control (CNC) machine as a tool to draw the stego signature (s) on the paper.
5. Testing and evaluating the result, can be based on the human vision as well as machine learning classifier such as neural network (NN)
6. The stego key (k) of the proposed steganography technique is assumed to be delivered to the recipient through a secure channel.

1.6 Thesis organization

The organization of the rest of the dissertation is as follows. Chapter two presents review of some of the theoretical and empirical literature on the information hiding, steganography, embedding approaches within digital media and respective steganalysis approaches, signature dataset, signature verification as well as signature synthesis. Chapter three describes the research methodology, in term of exploring the intra-user variability to hide the secret message (m) using human signature. In chapter four, the results attained in this study are presented and discussed. Finally, chapter five provides the conclusion as well as recommendations for the future works.

REFERENCES

Aabed, M. A., Awaideh, S. M., Rahman, A.-, Elshafei, M., & Gutub, A. A. (2007). Arabic Diacritics Based Steganography. Retrieved from https://eprints.kfupm.edu.sa/153/1/S.pdf

Abdulkader, H., & Roviras, D. (2012). Generating cryptography keys using self-organizing maps. In *2012 International Symposium on Wireless Communication Systems (ISWCS)* (pp. 736–740). IEEE. https://doi.org/10.1109/ISWCS.2012.6328465

Abdullah I. Al-Shoshan. (n.d.). Handwritten Signature Verification Using Image Invariants and Dynamic Features. In *International Conference on Computer Graphics, Imaging and Visualisation (CGIV'06)* (pp. 173–176). IEEE. https://doi.org/10.1109/CGIV.2006.52

Agarwal, M. (2013). TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON. *International Journal of Network Security & Its Applications (IJNSA)*, *5*(1). https://doi.org/10.5121/ijnsa.2013.5107

Ahmad, T., Sukanto, G., Studiawan, H., Wibisono, W., & Ijtihadie, R. M. (2014). Emoticon-based steganography for securing sensitive data. In *2014 6th International Conference on Information Technology and Electrical Engineering (ICITEE)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICITEED.2014.7007904

Ahmed, K., El-Henawy, I. M., Rashad, M. Z., & Nomir, O. (2010). On-line signature verification based on PCA feature reduction and statistical analysis. In *The 2010 International Conference on Computer Engineering & Systems* (pp. 3–8). IEEE. https://doi.org/10.1109/ICCES.2010.5674907

AL-Ani, Z. K., Zaidan, A. A., Zaidan, B. B., & Alanazi, H. O. (2010). Overview: Main Fundamentals for Steganography. Retrieved from http://arxiv.org/abs/1003.4086

Al-Ataby, A., & Al-Naima, F. (2010). A Modified High Capacity Image Steganography Technique Based on Wavelet Transform. *The International Arab Journal of Information Technology*, *7*(4). Retrieved from http://ccis2k.org/iajit/PDF/vol.7,no.4/730final.pdf

Al-Haidari, F., Gutub, A., Al-Kahsah, K., & Hamodi, J. (2009). Improving security and capacity for Arabic text steganography using "Kashida" extensions. In *2009 IEEE/ACS International Conference on Computer Systems and Applications* (pp. 396–399). IEEE. https://doi.org/10.1109/AICCSA.2009.5069355

Al-Mohammad, A., & Adel. (2010). Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility. Retrieved from http://bura.brunel.ac.uk/handle/2438/4634

Al-Othmani, A. Z., Manaf, A. A., Zeki, A. M., & Lumpur, K. (n.d.). A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation. Retrieved from https://pdfs.semanticscholar.org/2ea8/c2c1278d4e301da39f8b20816a7bfa76d442.pdf

Alameti, S., Pothalaiah, S., & Babu, D. . A. (2010). A New Approach to Telugu Text Steganography by Shifting Inherent Vowel Signs. *Networking and Communication Engineering*, *2*(11), 444–448. Retrieved from http://www.ciitresearch.org/dl/index.php/nce/article/view/NCE112010002

Alattar, A. M., & Alattar, O. M. (2004). Watermarking electronic text documents containing justified paragraphs and irregular line spacing. In E. J. Delp III & P. W. Wong (Eds.) (Vol. 5306, p. 685). International Society for Optics and Photonics. https://doi.org/10.1117/12.527147

Ali, A. E. (2010). A New Text Steganography Method By Using Non-Printing Unicode Characters. *Journal*, *28*(1). Retrieved from https://pdfs.semanticscholar.org/3f8d/a80fd500e27bb421e82ed7dccd172edaf9bf.pdf

Alla, K., & Prasad, R. S. R. (2009). An Evolution of Hindi Text Steganography. In *2009 Sixth International Conference on Information Technology: New Generations* (pp. 1577–1578). IEEE. https://doi.org/10.1109/ITNG.2009.41

Almohammad, A., & Ghinea, G. (2010). Stego image quality and the reliability of PSNR. In *2010 2nd International Conference on Image Processing Theory, Tools and Applications* (pp. 215–220). IEEE. https://doi.org/10.1109/IPTA.2010.5586786

Alonso-Fernandez, F., Fierrez-Aguilar, J., & Ortega-Garcia, J. (2005). Sensor Interoperability and Fusion in Signature Verification: A Case Study Using Tablet PC (pp. 180–187). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11569947_23

Altun, O., Sharma, G., Celik, M., Sterling, M., Titlebaum, E., & Bocko, M. (2005). Morphological Steganalysis of Audio Signals and the Principle of Diminishing Marginal Distortions. In *Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.* (Vol. 2, pp. 21–24). IEEE. https://doi.org/10.1109/ICASSP.2005.1415331

Alturki, F., & Mersereau, R. (2001). Secure blind image steganographic technique using discrete Fourier transformation. In *Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205)* (Vol. 2, pp. 542–545). Thessaloniki, Greece: IEEE. https://doi.org/10.1109/ICIP.2001.958548

Alves, D. K., Neto, C. M. S., Costa, F. B., & Ribeiro, R. L. A. (2014). Power measurement using the maximal overlap discrete wavelet transform. In *2014 11th IEEE/IAS International Conference on Industry Applications* (pp. 1–7). IEEE. https://doi.org/10.1109/INDUSCON.2014.7059455

Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. (2003). Information hiding using steganography. In *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.* (pp. 21–25). Shah Alam, Malaysia: IEEE. https://doi.org/10.1109/NCTT.2003.1188294

Amin Seyyedi, S., Sadau, V., & Ivanov, N. (2016). A Secure Steganography Method Based on Integer Lifting Wavelet Transform. *International Journal of Network Security*, *18*(1), 124–132. Retrieved from http://ijns.jalaxy.com.tw/contents/ijns-v18-n1/ijns-2016-v18-n1-p124-132.pdf

Amirtharaj, R., & Bosco Bala, J. (2012). Inverted Pattern in Inverted Time Domain for Icon Steganography. *Information Technology Journal*, *11*(5), 587–595. https://doi.org/10.3923/itj.2012.587.595

Anderson, R. J., & Petitcolas, F. A. P. (1998). On The Limits of Steganography. *IEEE Journal of Selected Areas in Communications*, *16*(4), 474–481. Retrieved from https://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf

Ansari, R., Malik, H., & Khokhar, A. (2004). Data-hiding in audio using frequency-selective phase alteration. *Unknown Journal*, *5*. Retrieved from https://experts.umich.edu/en/publications/data-hiding-in-audio-using-frequency-selective-phase-alteration

Antoniadis, A., & Oppenheim, G. (Eds.). (1995). *Wavelets and Statistics* (Vol. 103). New York, NY: Springer New York. https://doi.org/10.1007/978-1-4612-2544-7

Armand, S., Blumenstein, M., & Muthukkumarasamy, V. (2006). Off-line Signature Verification based on the Modified Direction Feature. In *18th International Conference on Pattern Recognition (ICPR'06)* (pp. 509–512). IEEE. https://doi.org/10.1109/ICPR.2006.893

Arora, M., Singh, K., & Mander, G. (2014). Discrete fractional cosine transform based online handwritten signature verification. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)* (pp. 1–6). IEEE.

https://doi.org/10.1109/RAECS.2014.6799647

Artz, D. (2001). Digital steganography: hiding data within data. *IEEE Internet Computing*, *5*(3), 75–80. https://doi.org/10.1109/4236.935180

Ashiq JA. (2015). Will Quantum Computers Threaten Modern Cryptography? Retrieved April 8, 2018, from https://www.tripwire.com/state-of-security/featured/will-quantum-computers-threaten-modern-cryptography/

Atallah, M. J., McDonough, C. J., Raskin, V., & Nirenburg, S. (2000). Natural language processing for information assurance and security. In *Proceedings of the 2000 workshop on New security paradigms - NSPW '00* (pp. 51–65). New York, New York, USA: ACM Press. https://doi.org/10.1145/366173.366190

Atallah, M. J., Raskin, V., Crogan, M., Hempelmann, C., Kerschbaum, F., Mohamed, D., & Naik, S. (2001). Natural Language Watermarking: Design, Analysis, and a Proof-of-Concept Implementation (pp. 185–200). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45496-9_14

Avcibas, I., Memon, N., & Sankur, B. (2003). Steganalysis using image quality metrics. *IEEE Transactions on Image Processing*, *12*(2), 221–229. https://doi.org/10.1109/TIP.2002.807363

Avcibas, I., Nasir, M., & Sankur, B. (n.d.). Steganalysis based on image quality metrics. In *2001 IEEE Fourth Workshop on Multimedia Signal Processing (Cat. No.01TH8564)* (pp. 517–522). IEEE. https://doi.org/10.1109/MMSP.2001.962785

Avcıbas, I. (2006). Audio Steganalysis With Content-Independent Distortion Measures. *IEEE Processing Letters*, *13*(2). Retrieved from https://pdfs.semanticscholar.org/bba2/5b95024565210d589597fd9206771c181b1c.pdf

Avcıbaş, İ., Kharrazi, M., Memon, N., & Sankur, B. (2005). Image Steganalysis with Binary Similarity Measures. *EURASIP Journal on Advances in Signal Processing*, *2005*(17), 679350. https://doi.org/10.1155/ASP.2005.2749

Badr, S. M., Selim, G. M. I., & Khalil, A. H. (2014). A Review on Steganalysis Techniques: From Image Format Point of View. *International Journal of Computer Applications*, *102*(4), 975–8887. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=18455F3361EC3FBD0717D1C83BAFBC33?doi=10.1.1.736.6450&rep=rep1&type=pdf

Bahi, J. M., Couchot, J.-F., & Guyeux, C. (2011). Steganography: a class of secure and robust algorithms. Retrieved from http://arxiv.org/abs/1112.1260

Bailey, K., Curran, K., & Condell, J. (2004). Evaluation of pixel-based steganography and stegodetection methods. *The Imaging Science Journal*, *52*(3), 131–150. https://doi.org/10.1179/136821904225020249

Balbed, M. A. M., Ahmad, S. M. S., & Shakil, A. (2009). ANOVA-based feature analysis and selection in HMM-based offline signature verification system. In *2009 Innovative Technologies in Intelligent Systems and Industrial Applications* (pp. 66–69). IEEE. https://doi.org/10.1109/CITISIA.2009.5224240

Ballard, L., Lopresti, D., & Monrose, F. (2007). Forgery Quality and Its Implications for Behavioral Biometric Security. *IEEE Transactions on Systems, Man and Cybernetics, Part B (Cybernetics)*, *37*(5), 1107–1118. https://doi.org/10.1109/TSMCB.2007.903539

Bandyopadhyay, S. K., Kim, T.-H., & Parui, S. (2011). Network Based Public Key Method for Steganography. In *2011 International Conference on Ubiquitous Computing and Multimedia Applications* (pp. 53–56). IEEE. https://doi.org/10.1109/UCMA.2011.19

Banerjee, I., Bhattacharyya, S., & Sanyal, G. (2013). Study and Analysis of Text Steganography Tools. *International Journal of Computer Network and Information Security*, *5*(12), 45–52. https://doi.org/10.5815/ijcnis.2013.12.06

Bassil, Y. (2012). A Two Intermediates Audio Steganography Technique. Retrieved from http://arxiv.org/abs/1212.2207

Bassil, & Youssef. (2014). *International Journal of Latest Trend in Computing IJLTC. International Journal of Latest Trends in Computing* (Vol. 4). Retrieved from http://ojs.excelingtech.co.uk/index.php/IJLTC/article/view/646

Bateman, P., & Schaathun, H. G. (2008). *Image Steganography and Steganalysis*. University of Surrey. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.449.2082&rep=rep1&type=pdf

Bennett, K. (n.d.). LINGUISTIC STEGANOGRAPHY: SURVEY, ANALYSIS, AND ROBUSTNESS CONCERNS FOR HIDING INFORMATION IN TEXT Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text. Retrieved from https://pdfs.semanticscholar.org/9ea2/84ed75ef281b3f53dae5951f5f00d86475dc.pdf

Bennett, K. (2004). Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text. Retrieved from https://pdfs.semanticscholar.org/9ea2/84ed75ef281b3f53dae5951f5f00d86475d

c.pdf

Bensaad, M. L., & Yagoubi, M. B. (2011). High capacity diacritics-based method for information hiding in Arabic text. In *2011 International Conference on Innovations in Information Technology* (pp. 433–436). IEEE. https://doi.org/10.1109/INNOVATIONS.2011.5893864

Bhattacharya, T., Dey, N., & Chaudhuri, S. R. B. (2012). A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum. Retrieved from http://arxiv.org/abs/1209.0054

Bhattacharyya, S., Banerjee, I., & Sanyal, G. (2011). A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier. *Journal of Global Research in Computer Science*, *2*(4). Retrieved from https://pdfs.semanticscholar.org/4d9e/ed31e55f9a557b46d4b30c6653d816bf3ec6.pdf

Bilal, M., Imtiaz, S., Abdul, W., & Ghouzali, S. (2013). Zero-steganography using DCT and spatial domain. In *2013 ACS International Conference on Computer Systems and Applications (AICCSA)* (pp. 1–7). IEEE. https://doi.org/10.1109/AICCSA.2013.6616431

Bilal, M., Imtiaz, S., Abdul, W., Ghouzali, S., & Asif, S. (2014). Chaos based Zero-steganography algorithm. *Multimedia Tools and Applications*, *72*(2), 1073–1092. https://doi.org/10.1007/s11042-013-1415-y

Bisla, N., & Chaudhary, P. (2013). Comparative Study of DWT and DWT-SVD Image Watermarking Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(6), 2277–128. Retrieved from https://pdfs.semanticscholar.org/e942/ec2c416c998e01a6138d994333c7dea3d43a.pdf

Blahut, R. E. (2014). *Cryptography and Secure Communication*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139013673

Böhme, R., & Ker, A. D. (2006). A Two-Factor Error Model for Quantitative Steganalysis. Retrieved from http://www.cs.ox.ac.uk/andrew.ker/docs/ADK15B-rev.pdf

Brassil, J., Low, S., Maxemchuk, N., & O'Gorman, L. (n.d.). Electronic marking and identification techniques to discourage document copying. In *Proceedings of INFOCOM '94 Conference on Computer Communications* (pp. 1278–1287). IEEE Comput. Soc. Press. https://doi.org/10.1109/INFCOM.1994.337544

Bunke, H., Jiang, X., Abegglen, K., & Kandel, A. (2002). On the Weighted Mean of a Pair of Strings. *Pattern Analysis & Applications*, *5*(1), 23–30. https://doi.org/10.1007/s100440200003

Cachin, C. (2004). An information-theoretic model for steganography. *Information and Computation*, *192*(1), 41–56. https://doi.org/10.1016/J.IC.2004.02.003

Cetin, O., & Ozcerit, A. T. (2009). A new steganography algorithm based on color histograms for data embedding into raw video streams. *Computers & Security*, *28*(7), 670–682. https://doi.org/10.1016/J.COSE.2009.04.002

Chadha, A., Satam, N., & Sood, R. (2013). An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution. *International Journal of Computer Applications*, *77*(13), 975–8887. Retrieved from https://pdfs.semanticscholar.org/10da/a4a777587fd1b2652bbc6f4988448ced2633.pdf

Chan Wai, E. N., & Khine, M. A. (2011). Modified Linguistic Steganography Approach by Using Syntax Bank and Digital Signature. *International Journal of Information and Education Technology*, *1*(5). Retrieved from https://pdfs.semanticscholar.org/1af9/289a968856d43339bd431368dc7b88e6df63.pdf

Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography techniques. In *Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205)* (Vol. 2, pp. 1019–1022). Thessaloniki, Greece: IEEE. https://doi.org/10.1109/ICIP.2001.958299

Chang, C.-C., Lin, C.-Y., & Wang, Y.-Z. (2006). New image steganographic methods using run-length approach. *Information Sciences*, *176*(22), 3393–3408. https://doi.org/10.1016/J.INS.2006.02.008

Chang, C.-Y., & Clark, S. (2010). Linguistic Steganography Using Automatically Generated Paraphrases, 591–599. Retrieved from http://www.aclweb.org/anthology/N10-1084

Changder, S., Das, S., & Ghosh, D. (2010). Text steganography through Indian languages using feature coding method. In *2010 2nd International Conference on Computer Technology and Development* (pp. 501–505). IEEE. https://doi.org/10.1109/ICCTD.2010.5645849

Changder, S., Debnath, N. C., & Ghosh, D. (2009). A New Approach to Hindi Text Steganography by Shifting Matra. In *2009 International Conference on Advances in Recent Technologies in Communication and Computing* (pp. 199–202). IEEE. https://doi.org/10.1109/ARTCom.2009.122

Chapman, M., Davida, G. I., & Rennhard, M. (2001). A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography (pp. 156–165). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45439-X_11

Charkari, N. M., & Chahooki, M. A. Z. (2007). A Robust High Capacity Watermarking Based on DCT and Spread Spectrum. In *2007 IEEE International Symposium on Signal Processing and Information Technology* (pp. 194–197). IEEE. https://doi.org/10.1109/ISSPIT.2007.4458077

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, *90*(3), 727–752. https://doi.org/10.1016/J.SIGPRO.2009.08.010

Chen, G., Chen, Q., Zhang, D., & Zhu, W. (2012). Particle Swarm Optimization Feature Selection for Image Steganalysis. In *2012 Fourth International Conference on Digital Home* (pp. 304–308). IEEE. https://doi.org/10.1109/ICDH.2012.28

Chen, P.-Y., & Lin, H.-J. (2006). A DWT Based Approach for Image Steganography. *International Journal of Applied Science and Engineering Int. J. Appl. Sci. Eng*, *4*(4), 275–290. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.499.1608&rep=rep1&type=pdf

Chen, W. (2005). *STUDY OF STEGANALYSIS METHODS*. New Jersey's Science and Technology University. Retrieved from http://archives.njit.edu/vol01/etd/2000s/2005/njit-etd2005-006/njit-etd2005-006.pdf

Chen, Z., Huang, L., Meng, P., Yang, W., & Miao, H. (2011). Blind Linguistic Steganalysis against Translation Based Steganography (pp. 251–265). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-18405-5_21

Chen, Z., Huang, L., Yu, Z., Yang, W., Li, L., Zheng, X., & Zhao, X. (2008). Linguistic Steganography Detection Using Statistical Characteristics of Correlations between Words (pp. 224–235). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88961-8_16

Chhikara, R., & Singh, L. (2013). A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted. *International Journal of Engineering and Innovative Technology (IJEIT)*, *3*(4). Retrieved from https://www.semanticscholar.org/paper/A-Review-on-Digital-Image-Steganalysis-Techniques-Chhikara-Singh/a53a6a0fdba923272333a1079114d02cf65ba2282

Cho, S., Cha, B.-H., Wang, J., & Kuo, C.-C. J. (2010). Block-based image steganalysis: Algorithm and performance evaluation. In *Proceedings of 2010 IEEE International Symposium on Circuits and Systems* (pp. 1679–1682). IEEE. https://doi.org/10.1109/ISCAS.2010.5537499

Çivicioğlu, P., Alçı, M., & Beşdok, E. (2004). Impulsive Noise Suppression from Images with the Noise Exclusive Filter. *EURASIP Journal on Advances in Signal Processing*, *2004*(16), 181785. https://doi.org/10.1155/S1110865704403151

Coetzer, J., Herbst, B. M., & du Preez, J. A. (2004). Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model. *EURASIP Journal on Advances in Signal Processing*, *2004*(4), 925026. https://doi.org/10.1155/S1110865704309042

Coifman, R. R., & Donoho, D. L. (1995). Translation-Invariant De-Noising (pp. 125–150). Springer, New York, NY. https://doi.org/10.1007/978-1-4612-2544-7_9

Cole, E. (2003). *Hiding in plain sight : steganography and the art of covert communication*. Wiley Pub.

Conway, M. (2003). Code wars: Steganography, signals intelligence, and terrorism. *Knowledge, Technology & Policy*, *16*(2), 45–62. https://doi.org/10.1007/s12130-003-1026-4

Cootes, T. F., Taylor, C. J., Cooper, D. H., & Graham, J. (1995). Active Shape Models-Their Training and Application. *Computer Vision and Image Understanding*, *61*(1), 38–59. https://doi.org/10.1006/CVIU.1995.1004

Cornish, C. R., Bretherton, C. S., & Percival, D. B. (2006). Maximal Overlap Wavelet Statistical Analysis With Application to Atmospheric Turbulence. *Boundary-Layer Meteorology*, *119*(2), 339–374. https://doi.org/10.1007/s10546-005-9011-y

Cox, I. J. (Ingemar J. . (2008). *Digital watermarking and steganography*. Morgan Kaufmann Publishers.

Crane, H. D., & Ostrem, J. S. (1983). Automatic signature verification using a three-axis force-sensitive pen. *IEEE Transactions on Systems, Man, and Cybernetics*, *SMC-13*(3), 329–337. https://doi.org/10.1109/TSMC.1983.6313165

Cusack, B., & Chambers, J. (2014). Detecting covert communication channels in raster images. *Australian Information Warfare and Security Conference*. https://doi.org/10.4225/75/57a84c3abefba

Cvejic, N., & Seppanen, T. (2002). Increasing the capacity of LSB-based audio steganography. In *2002 IEEE Workshop on Multimedia Signal Processing.* (pp. 336–338). St.Thomas, VI, USA: IEEE. https://doi.org/10.1109/MMSP.2002.1203314

Das, S., Das, S., Bandyopadhyay, B., & Sanyal, S. (2011). Steganography and Steganalysis: Different Approaches. Retrieved from http://arxiv.org/abs/1111.3758

Daubechies, I. (1988). Orthonormal bases of compactly supported wavelets. *Communications on Pure and Applied Mathematics*, *41*(7), 909–996. https://doi.org/10.1002/cpa.3160410705

Daugman, J. (2004). How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 21–30. https://doi.org/10.1109/TCSVT.2003.818350

Daugman, J., Adler, A., Schuckers, S., Nandakumar, K., Kennell, L. R., Rakvic, R. N., … Sankaranarayanan, A. C. (2009). Signature Sample Synthesis. In *Encyclopedia of Biometrics* (pp. 1205–1210). Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-73003-5_7

de Oliveira, C., A Kaestner, C., Bortolozzi, F., & Sabourin, R. (1997). Generation of signatures by deformations (pp. 283–298). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-63791-5_22

Deore, M. R., & Handore, S. M. (2015). A survey on offline signature recognition and verification schemes. In *2015 International Conference on Industrial Instrumentation and Control (ICIC)* (pp. 165–169). IEEE. https://doi.org/10.1109/IIC.2015.7150731

Di Lecce, V., Dimauro, G., Guerriero, A., Impedovo, S., Pirlo, G., Salzo, A., & Sarcinella, L. (1999). Selection of reference signatures for automatic signature verification. In *Proceedings of the Fifth International Conference on Document Analysis and Recognition. ICDAR '99 (Cat. No.PR00318)* (pp. 597–600). IEEE. https://doi.org/10.1109/ICDAR.1999.791858

Diaz-Cabrera, M., Ferrer, M. A., & Morales, A. (2014). Cognitive Inspired Model to Generate Duplicated Static Signature Images. In *2014 14th International Conference on Frontiers in Handwriting Recognition* (pp. 61–66). IEEE. https://doi.org/10.1109/ICFHR.2014.18

Diaz-Cabrera, M., Gomez-Barrero, M., Morales, A., Ferrer, M. A., & Galbally, J. (2014). Generation of Enhanced Synthetic Off-Line Signatures Based on Real On-Line Data. In *2014 14th International Conference on Frontiers in*

Handwriting Recognition (pp. 482–487). IEEE. https://doi.org/10.1109/ICFHR.2014.87

DIMAURO, G., IMPEDOVO, S., & PIRLO, G. (1994). COMPONENT-ORIENTED ALGORITHMS FOR SIGNATURE VERIFICATION. *International Journal of Pattern Recognition and Artificial Intelligence*, *8*(3), 771–793. https://doi.org/10.1142/S0218001494000401

Dimauro, G., Impedovo, S., Pirlo, G., & Salzo, A. (1997). A Multi-Expert Signature Verification System for Bankcheck Processing. *International Journal of Pattern Recognition and Artificial Intelligence*, *11*(5), 827–844. https://doi.org/10.1142/S0218001497000378

Din, R., Samsudin, A., T. Muda, T. Z., Lertkari, P., Ampahawan, A., & Omar, M. N. (2012). *Text steganalysis using evolution algorithm approach*. Retrieved from http://repo.uum.edu.my/10142/

Din, R., Samsudin, A., T. Muda, T. Z., Lertkari, P., Ampahawan, A., & Omar, M. N. (2013). Fitness Value Based Evolution Algorithm Approach for Text Steganalysis Model. *INTERNATIONAL JOURNAL OF MATHEMATICAL MODELS AND METHODS IN APPLIED SCIENCES*. Retrieved from https://pdfs.semanticscholar.org/3bd3/c40bd59f830afafc96074e3477c4beaef47e.pdf

Ding Huang, & Hong Yan. (2001). Interword distance changes represented by sine waves for watermarking text images. *IEEE Transactions on Circuits and Systems for Video Technology*, *11*(12), 1237–1245. https://doi.org/10.1109/76.974678

Djebbar, F., Ayad, B., Abed-Meraim, K., & Hamam, H. (2013). Unified phase and magnitude speech spectra data hiding algorithm. *Security and Communication Networks*, *6*(8), 961–971. https://doi.org/10.1002/sec.644

Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2012). Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, and Music Processing*, *2012*(1), 25. https://doi.org/10.1186/1687-4722-2012-25

Djioua, M., O'Reilly, C., & Plamondon, R. (2006). An interactive trajectory synthesizer to study outlier patterns in handwriting recognition and signature verification. In *18th International Conference on Pattern Recognition (ICPR'06)* (pp. 1124–1127). IEEE. https://doi.org/10.1109/ICPR.2006.256

Doddington, G., Doddington, G., Liggett, W., Martin, A., Przybocki, M., & Reynolds, D. (1998). SHEEP, GOATS, LAMBS and WOLVES A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation. *INTERNATIONAL CONFERENCE ON SPOKEN LANGUAGE PROCESSING*.

Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.61.2800

Drouhard, J.-P., Sabourin, R., & Godbout, M. (1996). A neural network approach to off-line signature verification using directional PDF. *Pattern Recognition*, *29*(3), 415–424. https://doi.org/10.1016/0031-3203(95)00092-5

Dunbar, B. (2002). A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment. Retrieved from https://www.sans.org/reading-room/whitepapers/covert/detailed-steganographic-techniques-open-systems-environment-677

Enqi, Z., Jinxu, G., Jianbin, Z., Chan, M., & Linjuan, W. (2009). On-line Handwritten Signature Verification Based on Two Levels Back Propagation Neural Network. In *2009 International Symposium on Intelligent Ubiquitous Computing and Education* (pp. 202–205). IEEE. https://doi.org/10.1109/IUCE.2009.142

Fahmy, M. M. M. (2010). Online handwritten signature verification system based on DWT features extraction and neural network classification. *Ain Shams Engineering Journal*, *1*(1), 59–70. https://doi.org/10.1016/J.ASEJ.2010.09.007

Fairhust, M. C., & Ng, S. (n.d.). Management of access through biometric control: A case study based on automatic signature verification. *Universal Access in the Information Society*, *1*(1), 31–39. https://doi.org/10.1007/s102090100009

Fang, B., Leung, C. H., & Tang, Y. Y. (2002). Off-line signature verification with generated training samples. In G. Mu, F. T. S. Yu, & S. Jutamulia (Eds.) (Vol. 4929, pp. 388–397). International Society for Optics and Photonics. https://doi.org/10.1117/12.483241

Fang, B., Leung, C. H., Tang, Y. Y., Tse, K. W., Kwok, P. C. K., & Wong, Y. K. (2003). Off-line signature verification by the tracking of feature and stroke positions. *Pattern Recognition*, *36*(1), 91–101. https://doi.org/10.1016/S0031-3203(02)00061-4

Faria Costa, L., & Paschoarelli Veiga, A. C. (2005). Identification of the best quantization table using genetic algorithms. In *PACRIM. 2005 IEEE Pacific Rim Conference on Communications, Computers and signal Processing, 2005.* (pp. 570–573). IEEE. https://doi.org/10.1109/PACRIM.2005.1517353

Farid, H. (2003). DETECTING HIDDEN MESSAGES USING HIGHER-ORDER STATISTICAL MODELS. Retrieved from http://www.cs.dartmouth.edu/farid/downloads/publications/icip02.pdf

Feng, H., & Wah, C. C. (2003). Online signature verification using a new extreme points warping technique. *Pattern Recognition Letters*, *24*(16), 2943–2951. https://doi.org/10.1016/S0167-8655(03)00155-7

Ferrer, M. A., Alonso, J. B., & Travieso, C. M. (2005). Offline geometric parameters for automatic signature verification using fixed-point arithmetic. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *27*(6), 993–997. https://doi.org/10.1109/TPAMI.2005.125

Ferrer, M. A., Diaz-Cabrera, M., & Morales, A. (2013). Synthetic off-line signature image generation. In *2013 International Conference on Biometrics (ICB)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICB.2013.6612969

Ferrer, M. A., Diaz-Cabrera, M., & Morales, A. (2015). Static Signature Synthesis: A Neuromotor Inspired Approach for Biometrics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *37*(3), 667–680. https://doi.org/10.1109/TPAMI.2014.2343981

Ferrer, M. A., Diaz-Cabrera, M., Morales, A., Galbally, J., & Gomez-Barrero, M. (2013). Realistic synthetic off-line signature generation based on synthetic on-line data. In *2013 47th International Carnahan Conference on Security Technology (ICCST)* (pp. 1–6). IEEE. https://doi.org/10.1109/CCST.2013.6922041

Foroozandeh, A., Akbari, Y., Jalili, M. J., & Sadri, J. (2012). Persian Signature Verification Based on Fractal Dimension Using Testing Hypothesis. In *2012 International Conference on Frontiers in Handwriting Recognition* (pp. 313–318). IEEE. https://doi.org/10.1109/ICFHR.2012.254

Frias-Martinez, E., Sanchez, A., & Velez, J. (2006). Support vector machines versus multi-layer perceptrons for efficient off-line signature recognition. *Engineering Applications of Artificial Intelligence*, *19*(6), 693–704. https://doi.org/10.1016/J.ENGAPPAI.2005.12.006

Fridrich, J., Goljan, M., & Du, R. (n.d.). Reliable Detection of LSB Steganography in Color and Grayscale Images. Retrieved from http://www.ws.binghamton.edu/fridrich/Research/acm_2001_03.pdf

Fuentes, M., Garcia-Salicetti, S., & Dorizzi, B. (n.d.). On line signature verification: Fusion of a Hidden Markov Model and a neural network via a support vector machine. In *Proceedings Eighth International Workshop on Frontiers in Handwriting Recognition* (pp. 253–258). IEEE Comput. Soc. https://doi.org/10.1109/IWFHR.2002.1030918

Galbally, J., Fierrez, J., Martinez-Diaz, M., & Ortega-Garcia, J. (2009a). Evaluation of Brute-force Attack to Dynamic Signature Verification Using Synthetic Samples. In *2009 10th International Conference on Document Analysis and Recognition* (pp. 131–135). IEEE. https://doi.org/10.1109/ICDAR.2009.39

Galbally, J., Fierrez, J., Martinez-Diaz, M., & Ortega-Garcia, J. (2009b). Improving the Enrollment in Dynamic Signature Verfication with Synthetic Samples. In *2009 10th International Conference on Document Analysis and Recognition* (pp. 1295–1299). IEEE. https://doi.org/10.1109/ICDAR.2009.38

Galbally, J., Fierrez, J., Ortega-Garcia, J., & Plamondon, R. (2012). Synthetic on-line signature generation. Part II: Experimental validation. *Pattern Recognition*, *45*(7), 2622–2632. https://doi.org/10.1016/J.PATCOG.2011.12.007

Galbally, J., Galbally, J., Fierrez, J., Martinez-diaz, M., & Ortega-garcia, J. (n.d.). Synthetic Generation of Handwritten Signatures Based on Spectral Analysis. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.186.1480

Galbally, J., Plamondon, R., Fierrez, J., & Ortega-Garcia, J. (2012). Synthetic on-line signature generation. Part I: Methodology and algorithms. *Pattern Recognition*, *45*(7), 2610–2621. https://doi.org/10.1016/J.PATCOG.2011.12.011

Garg, M. (2011). A Novel Text Steganography Technique Based on Html Documents. *International Journal of Advanced Science and Technology*, *35*. Retrieved from https://pdfs.semanticscholar.org/51cc/dc6e9801e8b37e7124ae3a9de13190bbedba.pdf

Gawor, P., & Koo Lodziej, J. (n.d.). An Application of Bezier curves in the off-line verification of handwritten signatures. Retrieved from https://troja.uksw.edu.pl/pdf/kaeiog/KAEiOG2007.11.pdf

Geetha, S., Ishwarya, N., & Kamaraj, N. (2010). Audio steganalysis with Hausdorff distance higher order statistics using a rule based decision tree paradigm. *Expert Systems with Applications*, *37*(12), 7469–7482. https://doi.org/10.1016/J.ESWA.2010.04.012

Ghasemzadeh, H., & Khalili arjmand, M. (2014). Reversed-Mel cepstrum based audio steganalysis - Semantic Scholar. In *4th International Conference on Computer and Knowledge Engineering (ICCKE*. Retrieved from https://www.semanticscholar.org/paper/Reversed-Mel-cepstrum-based-audio-steganalysis-Ghasemzadeh-Arjmandi/1388e0f6e975b04d47316be1b530d9c0f7a579f3

Gibbons, J. D., & Chakraborti, S. (2011). *Nonparametric statistical inference*. Chapman & Hall/Taylor & Francis. Retrieved from https://www.crcpress.com/Nonparametric-Statistical-Inference-Fifth-Edition/Gibbons-Chakraborti/p/book/9781420077612

Godhavari, T., Alamelu, N. R., & Soundararajan, R. (2005). Cryptography Using Neural Network. In *2005 Annual IEEE India Conference - Indicon* (pp. 258–261). Chennai, India: IEEE. https://doi.org/10.1109/INDCON.2005.1590168

Goh, S. S., Lim, Z. Y., & Shen, Z. (2006). Symmetric and antisymmetric tight wavelet frames. *Applied and Computational Harmonic Analysis*, *20*(3), 411–421. https://doi.org/10.1016/J.ACHA.2005.09.006

Goljan, M., Fridrich, J., & Cogranne, R. (2004). Rich Model for Steganalysis of Color Images. Retrieved from http://www.ws.binghamton.edu/fridrich/Research/color-04.pdf

Gopalan, K. (2005). Audio Steganography by Cepstrum Modification. In *Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.* (Vol. 5, pp. 481–484). IEEE. https://doi.org/10.1109/ICASSP.2005.1416345

Gopalan, K., Wenndt, S., Noga, A., Haddad, D., & Adams, S. (2003). Covert Speech Communication Via Cover Speech By Tone Insertion. Retrieved from https://pdfs.semanticscholar.org/c824/8bd4dc87c0e1b0da72060dda8260102dce42.pdf

Gope, P., Kumar, A., & Luthra, G. (2010). An Enhanced JPEG Steganography Scheme with Encryption Technique. *International Journal of Computer and Electrical Engineering*, *2*(5), 1793–8163. Retrieved from http://www.ijcee.org/papers/253-E676.pdf

Grgi, S., Grgi, M., & Mrak, M. (2004). RELIABILITY OF OBJECTIVE PICTURE QUALITY MEASURES. *Journal of ELECTRICAL ENGINEERING*, *55*(2), 3–10. Retrieved from https://pdfs.semanticscholar.org/7f67/518607121191dc3c3aa9d28f8db9ea96972a.pdf

Grosso, E., Pulina, L., & Tistarelli, M. (2012). Modeling biometric template update with Ant Colony Optimization. In *2012 5th IAPR International Conference on Biometrics (ICB)* (pp. 506–511). IEEE. https://doi.org/10.1109/ICB.2012.6199800

Gruber, C., Coduro, M., & Sick, B. (2006). Signature Verification with Dynamic RBF Networks and Time Series Motifs. Retrieved from https://hal.inria.fr/inria-00104508/en/

Gruber, C., Gruber, T., Krinninger, S., & Sick, B. (2010). Online Signature Verification With Support Vector Machines Based on LCSS Kernel Functions. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *40*(4), 1088–1100. https://doi.org/10.1109/TSMCB.2009.2034382

Gruhl, D., Lu, A., & Bender, W. (1996). Echo hiding (pp. 295–315). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-61996-8_48

Guest, R. M. (n.d.). The Repeatability of Signatures. In *Ninth International Workshop on Frontiers in Handwriting Recognition* (pp. 492–497). IEEE. https://doi.org/10.1109/IWFHR.2004.103

Gupta, N., & Sharma, N. (2014). Dwt and Lsb based Audio Steganography. In *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)* (pp. 428–431). IEEE. https://doi.org/10.1109/ICROIT.2014.6798368

Gupta, S., & Dhanda, N. (n.d.). Audio Steganography Using Discrete Wavelet Transformation (DWT) & Discrete Cosine Transformation (DCT). *IOSR Journal of Computer Engineering*, *17*(2), 2278–2661. https://doi.org/10.9790/0661-17253244

Gutierrez-Cardenas, J. M. (2014). Secret Key Steganography with Message Obfuscation by Pseudo-random Number Generators. In *2014 IEEE 38th International Computer Software and Applications Conference Workshops* (pp. 164–168). IEEE. https://doi.org/10.1109/COMPSACW.2014.31

Gutub, A. A.-A., & Mohammad Fattani, M. (2007). A Novel Arabic Text Steganography Method Using Letter Points and Extensions. *International Journal of Computer and Information Engineering*, *1*(3). Retrieved from https://waset.org/publications/5745/a-novel-arabic-text-steganography-method-using-letter-points-and-extensions-

Gutub, A. a, Ghouti, L. M., Elarian, Y. S., Awaideh, S. M., & Alvi, A. K. (2010). Utilizing Diacritics Marks for Arabic Text Steganography. *Kuwait Journal of Science & Engineering (KJSE)*, *37*(1), 89–109.

Guyon, I., Schomaker, L., Plamondon, R., Liberman, M., & Janet, S. (n.d.). UNIPEN project of on-line data exchange and recognizer benchmarks. In *Proceedings of the 12th IAPR International Conference on Pattern Recognition (Cat. No.94CH3440-5)* (Vol. 2, pp. 29–33). IEEE Comput. Soc. Press.

https://doi.org/10.1109/ICPR.1994.576870

Hansheng Lei, Palla, S., & Govindaraju, V. (2004). An Intuitive Similarity Measure for On-Line Signature Verification. In *Ninth International Workshop on Frontiers in Handwriting Recognition* (pp. 191–195). IEEE. https://doi.org/10.1109/IWFHR.2004.38

Harmsen, J. J., & Pearlman, W. A. (2004). Kernel Fisher discriminant for steganalysis of JPEG hiding methods. In E. J. Delp III & P. W. Wong (Eds.) (Vol. 5306, p. 13). International Society for Optics and Photonics. https://doi.org/10.1117/12.525996

Harralson, H. H. (2013). *Developments in handwriting and signature identification in the digital age*. Anderson. Retrieved from https://www.routledge.com/Developments-in-Handwriting-and-Signature-Identification-in-the-Digital/Harralson/p/book/9781455731473

Herbst, N. M., & Liu, C. N. (1977). Automatic Signature Verification Based on Accelerometry. *IBM Journal of Research and Development*, *21*(3), 245–253. https://doi.org/10.1147/rd.213.0245

Huang, D.-Y., & Yeo, T. Y. (2002). Robust and Inaudible Multi-echo Audio Watermarking (pp. 615–622). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36228-2_76

Huang, H.-J., Sun, X.-M., Sun, G., & Huang, J.-W. (2007). Detection of Hidden Information in Tags of Webpage Based on Tag-Mismatch. In *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)* (pp. 257–260). IEEE. https://doi.org/10.1109/IIHMSP.2007.4457539

Huang, H., Tan, J., Sun, X., & Liu, L. (2009). Detection of Hidden Information in Webpage Based on Higher-Order Statistics (pp. 293–302). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04438-0_25

Huang, K., & Yan, H. (1997). Off-line signature verification based on geometric feature extraction and neural network classification. *Pattern Recognition*, *30*(1), 9–17. https://doi.org/10.1016/S0031-3203(96)00063-5

Igarza, J. J., Goirizelaia, I., Espinosa, K., Hernáez, I., Méndez, R., & Sánchez, J. (2003). Online Handwritten Signature Verification Using Hidden Markov Models (pp. 391–399). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24586-5_48

Impedovo, D., & Pirlo, G. (2008). Automatic Signature Verification: The State of the Art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *38*(5), 609–635. https://doi.org/10.1109/TSMCC.2008.923866

Ioannidou, A., Halkidis, S. T., & Stephanides, G. (2012). A novel technique for image steganography based on a high payload method and edge detection. *Expert Systems with Applications*, *39*(14), 11517–11524. https://doi.org/10.1016/J.ESWA.2012.02.106

Iranmanesh, V., Ahmad, S. M. S., Adnan, W. A. W., Yussof, S., Arigbabu, O. A., & Malallah, F. L. (2014). Online handwritten signature verification using neural network classifier based on principal component analysis. *TheScientificWorldJournal*, *2014*, 381469. https://doi.org/10.1155/2014/381469

Islam, T., & Fairhurst, M. (2012). Natural Revocability in Handwritten Signatures to Enhance Biometric Security. In *2012 International Conference on Frontiers in Handwriting Recognition* (pp. 791–796). IEEE. https://doi.org/10.1109/ICFHR.2012.240

Jain, A., Bolle, R., & Pankanti, S. (n.d.). Introduction to Biometrics. In *Biometrics* (pp. 1–41). Boston, MA: Springer US. https://doi.org/10.1007/0-306-47044-6_1

Johnson, M. K., Lyu, S., & Farid, H. (2005). Steganalysis of Recorded Speech. Retrieved from http://www.ists.dartmouth.edu/library/28.pdf

Johnson, N. F., & Jajodia, S. (1998a). Exploring steganography: Seeing the unseen. *Computer*, *31*(2), 26–34. https://doi.org/10.1109/MC.1998.4655281

Johnson, N. F., & Jajodia, S. (1998b). Steganalysis of Images Created Using Current Steganography Software (pp. 273–289). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-49380-8_19

Johnson, N. F., & Katzenbeisser, S. C. (2000). *A survey of steganographic techniques*. Retrieved from https://pdfs.semanticscholar.org/00cc/e201016ba60bd89177a655b0f549b5454574.pdf

Juneja, M., & Sandhu, P. S. (2009). Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption. In *2009 International Conference on Advances in Recent Technologies in Communication and Computing* (pp. 302–305). IEEE. https://doi.org/10.1109/ARTCom.2009.228

Justino, E. J. R., Bortolozzi, F., & Sabourin, R. (2002). Off-line signature verification using HMM for random, simple and skilled forgeries. In *Proceedings of Sixth International Conference on Document Analysis and Recognition* (pp. 1031–

1034). IEEE Comput. Soc. https://doi.org/10.1109/ICDAR.2001.953942

Justino, E. J. R., Bortolozzi, F., & Sabourin, R. (2005). A comparison of SVM and HMM classifiers in the off-line signature verification. *Pattern Recognition Letters*, *26*(9), 1377–1385. https://doi.org/10.1016/J.PATREC.2004.11.015

Kahn, D. (1968). The Codebreakers. The Story of Secret Writing. In *Science* (Vol. 161, pp. 35–36). American Association for the Advancement of Science. https://doi.org/10.1126/science.161.3836.35-a

Kahn, D. (1996). The history of steganography (pp. 1–5). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-61996-8_27

Kaiyue Wang, Yunhong Wang, & Zhaoxiang Zhang. (2011). On-line signature verification using wavelet packet. In *2011 International Joint Conference on Biometrics (IJCB)* (pp. 1–6). IEEE. https://doi.org/10.1109/IJCB.2011.6117587

Kashi, R., Hu, J., Nelson, W. L., & Turin, W. (1998). A Hidden Markov Model approach to online handwritten signature verification. *International Journal on Document Analysis and Recognition*, *1*(2), 102–109. https://doi.org/10.1007/s100320050010

Kashi, R. S., Hu, J., Nelson, W. L., & Turin, W. (n.d.). On-line handwritten signature verification using hidden Markov model features. In *Proceedings of the Fourth International Conference on Document Analysis and Recognition* (Vol. 1, pp. 253–257). IEEE Comput. Soc. https://doi.org/10.1109/ICDAR.1997.619851

Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information hiding techniques for steganography and digital watermarking*. Artech House. Retrieved from https://dl.acm.org/citation.cfm?id=555654

Kaur, B., Kaur, A., & Singh, J. (2011). STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN. *International Journal of Advances in Engineering & Technology*, *1*(3), 2231–1963. Retrieved from https://pdfs.semanticscholar.org/70fb/f3b7946777a458b730a6b8791f74040c983b.pdf

Kaur, M., & Kaur, G. (2014). Review of Various Steganalysis Techniques. *International Journal of Computer Science and Information Technologies (IJCSIT)*, *5*(2). Retrieved from https://users.cs.fiu.edu/~fortega/df/research/Stenography II/review of various steganalyiss techniques.pdf

Kaur, R., & Choudhary, P. (2015). Offline Signature Verification in Punjabi based on SURF Features and Critical Point Matching using HMM. *International Journal of Computer Applications*, *111*(16), 4–11. https://doi.org/10.5120/19620-1288

Ker, A. D. (2006). Fourth-Order Structural Steganalysis and Analysis of Cover Assumptions. Retrieved from https://pdfs.semanticscholar.org/f6b1/4587e926943be714f5a8ee3bcdc814bd9575.pdf

Kexin, Z. (2010). Audio steganalysis of spread spectrum hiding based on statistical moment. In *2010 2nd International Conference on Signal Processing Systems* (pp. V3-381-V3-384). IEEE. https://doi.org/10.1109/ICSPS.2010.5555836

Khademi, M., & Ali Tinati, M. (2011). Audio steganography by using of linear predictive coding analysis in the safe places of discrete wavelet transform domain - Semantic Scholar. In *19th Iranian Conference on Electrical Engineering*. Retrieved from https://www.semanticscholar.org/paper/Audio-steganography-by-using-of-linear-predictive-Khademi-Tinati/6b3f7f50f26d6b79d95017f007001f49ad399b8a

Khalighi, S., Sousa, T., Oliveira, D., Pires, G., & Nunes, U. (2011). Efficient feature selection for sleep staging based on maximal overlap discrete wavelet transform and SVM. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (pp. 3306–3309). IEEE. https://doi.org/10.1109/IEMBS.2011.6090897

Kharrazi, M., Sencar, H. T., & Memon, N. (2004). Image Steganography: Concepts and Practice. Retrieved from http://isis.poly.edu/~steganography/pubs/ims04.pdf

Kholmatov, A., & Yanikoglu, B. (2005). Identity authentication using improved online signature verification method. *Pattern Recognition Letters*, *26*(15), 2400–2408. https://doi.org/10.1016/J.PATREC.2005.04.017

Kim, J., Yu, J. R., & Kim, S. H. (1996). Learning of prototypes and decision boundaries for a verification problem having only positive samples. *Pattern Recognition Letters*, *17*(7), 691–697. https://doi.org/10.1016/0167-8655(96)00016-5

Kipper, G. (2004). *Investigator's guide to steganography*. Auerbach Publications.

Kirovski, D., & Malvar, H. S. (2003). Spread-spectrum watermarking of audio signals. *IEEE Transactions on Signal Processing*, *51*(4), 1020–1033. https://doi.org/10.1109/TSP.2003.809384

Kodovský, J., & Fridrich, J. (2013). JPEG-Compatibility Steganalysis Using Block-Histogram of Recompression Artifacts (pp. 78–93). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-36373-3_6

Kraetzer, C., & Dittmann, J. (2007). Pros and cons of mel-cepstrum based audio steganalysis using SVM classification (pp. 359–377). Springer. Retrieved from https://dl.acm.org/citation.cfm?id=1782888

Kumar, A., & Pooja, K. (2010). Steganography- A Data Hiding Technique. *International Journal of Computer Applications*, *9*(7). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.206.5754

Kumar, S., & Banik, G. (2012). LSB Modification and Phase Encoding Technique of Audio Steganography Revisited. *International Journal of Advanced Research in Computer and Communication Engineering*, *1*(4). Retrieved from https://www.ijarcce.com/upload/june/11_LSB Modification and Phase Encoding Technique of Audio Steganography Revisited.pdf

Kumar Bandyopadhyay, S., & Parui, S. (2010). A Method for Public Key Method of Steganography. *International Journal of Computer Applications*, *6*(3), 975–8887. Retrieved from https://pdfs.semanticscholar.org/c6bb/ed59114bce710316da17ad4873d6ca7cee7e.pdf

Lee, J., Yoon, H.-S., Soh, J., Chun, B. T., & Chung, Y. K. (2004). Using geometric extrema for segment-to-segment characteristics comparison in online signature verification. *Pattern Recognition*, *37*(1), 93–103. https://doi.org/10.1016/S0031-3203(03)00229-2

Lee, L. L., & Berger, T. (n.d.). Reliable on-line human signature verification system for point-of-sales applications. In *Proceedings of the 12th IAPR International Conference on Pattern Recognition (Cat. No.94CH3440-5)* (Vol. 2, pp. 19–23). IEEE Comput. Soc. Press. https://doi.org/10.1109/ICPR.1994.576868

Lejtman, D. Z., & George, S. E. (n.d.). On-line handwritten signature verification using wavelets and back-propagation neural networks. In *Proceedings of Sixth International Conference on Document Analysis and Recognition* (pp. 992–996). IEEE Comput. Soc. https://doi.org/10.1109/ICDAR.2001.953934

Lew, J. S. (1980). Optimal Accelerometer Layouts for Data Recovery in Signature Verification. *IBM Journal of Research and Development*, *24*(4), 496–511. https://doi.org/10.1147/rd.244.0496

Leys, C., Ley, C., Klein, O., Bernard, P., & Licata, L. (2013). Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the

median. *Journal of Experimental Social Psychology*, *49*(4), 764–766. https://doi.org/10.1016/J.JESP.2013.03.013

Li, F., Zhang, X., Chen, B., & Feng, G. (2013). JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier. *IEEE Signal Processing Letters*, *20*(3), 233–236. https://doi.org/10.1109/LSP.2013.2240385

Li, H., Sun, Z., & Zhou, Z. (2011). An image steganalysis method based on characteristic function moments and PCA. In E. J. Delp III & P. W. Wong (Eds.). Yantai, China: IEEE. https://doi.org/10.1117/12.526012

Li, L., Huang, L., Zhao, X., Yang, W., & Chen, Z. (2008). A Statistical Attack on a Kind of Word-Shift Text-Steganography. In *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 1503–1507). IEEE. https://doi.org/10.1109/IIH-MSP.2008.42

Liang Zhang, Haili Wang, & Renbiao Wu. (2009). A High-Capacity Steganography Scheme for JPEG2000 Baseline System. *IEEE Transactions on Image Processing*, *18*(8), 1797–1803. https://doi.org/10.1109/TIP.2009.2021544

Liu, Q., Sung, A. H., & Qiao, M. (2008). Detecting information-hiding in WAV audios. In *2008 19th International Conference on Pattern Recognition* (pp. 1–4). IEEE. https://doi.org/10.1109/ICPR.2008.4761650

Liu, Q., Sung, A. H., & Qiao, M. (2009). Novel stream mining for audio steganalysis. In *Proceedings of the seventeen ACM international conference on Multimedia - MM '09* (p. 95). New York, New York, USA: ACM Press. https://doi.org/10.1145/1631272.1631288

Liu, T.-Y., & Tsai, W.-H. (2007). A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique. *IEEE Transactions on Information Forensics and Security*, *2*(1), 24–30. https://doi.org/10.1109/TIFS.2006.890310

Liu, Y., Chiang, K., Corbett, C., Archibald, R., Mukherjee, B., & Ghosal, D. (2008). A Novel Audio Steganalysis Based on High-Order Statistics of a Distortion Measure with Hausdorff Distance. In *Information Security* (pp. 487–501). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-85886-7_33

Liu Shaohui, Yao Hongxun, & Gao Wen. (2003). Neural network based steganalysis in still images. In *2003 International Conference on Multimedia and Expo. ICME '03. Proceedings (Cat. No.03TH8698)* (p. II-509). IEEE. https://doi.org/10.1109/ICME.2003.1221665

LORETTE, G., & PLAMONDON, R. (1990). DYNAMIC APPROACHES TO HANDWRITTEN SIGNATURE VERIFICATION. In *Computer Processing of Handwriting* (pp. 21–47). WORLD SCIENTIFIC. https://doi.org/10.1142/9789814439329_0002

Luo, X.-Y., Wang, D.-S., Wang, P., & Liu, F.-L. (2008). A review on blind detection for image steganography. *Signal Processing*, *88*(9), 2138–2157. https://doi.org/10.1016/J.SIGPRO.2008.03.016

Luo, X., Liu, B., & Liu, F. (2005). Improved RS Method for Detection of LSB Steganography (pp. 508–516). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11424826_54

Luo, X., Liu, F., Jianming Chen, & Yining Zhang. (2008). Image universal steganalysis based on wavelet packet transform. In *2008 IEEE 10th Workshop on Multimedia Signal Processing* (pp. 780–784). IEEE. https://doi.org/10.1109/MMSP.2008.4665180

Luo, X., Liu, F., & Lu, P. (2007). A LSB STEGANOGRAPHY APPROACH AGAINST PIXELS SAMPLE PAIRS STEGANALYSIS. *International Journal of Innovative Computing*, *3*(3), 575–588. Retrieved from https://pdfs.semanticscholar.org/4299/6852d7bdbccc3e71f8336ddcf6a970c5c8a2.pdf

Lyu, S., & Farid, H. (2004). Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines. Retrieved from www.cs.dartmouth.edu/~%7Blsw,farid%7D

Madasu, V. K., Yusof, M. H. M., Hanmandlu, M., & Kubik, K. (2003). Off-Line Signature Verification and Forgery Detection System Based on Fuzzy Modeling (pp. 1003–1013). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24581-0_86

Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., & Neri, A. (2010). Cancelable Templates for Sequence-Based Biometrics with Application to On-line Signature Recognition. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *40*(3), 525–538. https://doi.org/10.1109/TSMCA.2010.2041653

Majumder, A., & Changder, S. (2013). A Novel Approach for Text Steganography: Generating Text Summary Using Reflection Symmetry. *Procedia Technology*, *10*, 112–120. https://doi.org/10.1016/J.PROTCY.2013.12.343

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. London: Springer London. https://doi.org/10.1007/978-1-84882-

254-2

Mansfield, A. J., & Wayman, J. L. (2002). Best Practices in Testing and Reporting Performance of Biometric Devices. Retrieved from http://www.idsysgroup.com/ftp/BestPractice.pdf

Marcelli, A., Parziale, A., & Senatore, R. (n.d.). Some Observations on Handwriting from a Motor Learning Perspective. Retrieved from https://pdfs.semanticscholar.org/3c06/039b7a7e583cd489e745471bb7e389e650af.pdf

Marini, E., Autrusseau, F., Le Callet, P., & Campisi, P. (2008). Evaluation of standard watermarking techniques. Retrieved from https://hal.archives-ouvertes.fr/hal-00250682/document

Marius Iulian, M. (2013). Direct Problems and Inverse Problems in Biometric Systems. *Scientific Papers (Www.scientificpapers.org) Journal of Knowledge Management Economics and Information Technology*, *1*(5). Retrieved from http://www.scientificpapers.org/wp-content/files/1410_Mihailescu-Direct_Problems_and_Inverse_Problems_in_Biometric_Systems.pdf

Martens, R., & Claesen, L. (1996). On-line signature verification by dynamic time-warping. In *Proceedings of 13th International Conference on Pattern Recognition* (pp. 38–42 vol.3). IEEE. https://doi.org/10.1109/ICPR.1996.546791

Marvel, L. M., Boncelet, C. G., & Retter, C. T. (1998). Reliable Blind Information Hiding for Images (pp. 48–61). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-49380-8_4

Marvel, L. M., Boncelet, C. G., & Retter, C. T. (1999). Spread spectrum image steganography. *IEEE Transactions on Image Processing*, *8*(8), 1075–1083. https://doi.org/10.1109/83.777088

Matsuoka, H. (2006). Spread Spectrum Audio Steganography Using Sub-band Phase Shifting. In *2006 International Conference on Intelligent Information Hiding and Multimedia* (pp. 3–6). IEEE. https://doi.org/10.1109/IIH-MSP.2006.265106

McCabe, A., & Trevathan, J. (2008). Markov Model-Based Handwritten Signature Verification. In *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (pp. 173–179). IEEE. https://doi.org/10.1109/EUC.2008.138

Meghanathan, N., & Nayak, L. (2010). STEGANALYSIS ALGORITHMS FOR DETECTING THE HIDDEN INFORMATION IN IMAGE, AUDIO AND VIDEO COVER MEDIA. *International Journal of Network Security & Its*

Application (IJNSA), *2*(1). Retrieved from https://pdfs.semanticscholar.org/2724/3ae662027ff79607c556c3127a10e79461b9.pdf

Menezes, A. J. (Alfred J. ., Van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of applied cryptography*. CRC Press. Retrieved from http://cacr.uwaterloo.ca/hac/

Meng, P., Hang, L., Yang, W., Chen, Z., & Zheng, H. (2009). Linguistic Steganography Detection Algorithm Using Statistical Language Model. In *2009 International Conference on Information Technology and Computer Science* (pp. 540–543). IEEE. https://doi.org/10.1109/ITCS.2009.246

Mishra, M., Tiwari, G., & Yadav, A. K. (2014). Secret communication using Public Key steganography. In *International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICRAIE.2014.6909252

Mohamed, A. A. (2014). An improved algorithm for information hiding based on features of Arabic text: A Unicode approach. *Egyptian Informatics Journal*, *15*(2), 79–87. https://doi.org/10.1016/J.EIJ.2014.04.002

Morkel, T., Eloff, J. H. P., & Olivier, M. S. (2005). AN OVERVIEW OF IMAGE STEGANOGRAPHY. Retrieved from http://repository.root-me.org/Stéganographie/EN - Image Steganography Overview.pdf

Moulin, P., & Koetter, R. (2005). Data-Hiding Codes. *Proceedings of the IEEE*, *93*(12), 2083–2126. https://doi.org/10.1109/JPROC.2005.859599

Muda, L., Begam, M., & Elamvazuthi, I. (2010). Voice Recognition Algorithms using Mel Frequency Cepstral Coefficient (MFCC) and Dynamic Time Warping (DTW) Techniques. Retrieved from http://arxiv.org/abs/1003.4083

Mumtazah Syed Ahmad, S., Mohd Ali, B., & Azizun Wan Adnan, W. (2012). TECHNICAL ISSUES AND CHALLENGES OF BIOMETRIC APPLICATIONS AS ACCESS CONTROL TOOLS OF INFORMATION SECURITY. *International Journal of Innovative Computing*, *8*(11), 7983–7999. Retrieved from http://www.ijicic.org/ijicic-ksi-13.pdf

Munich, M. E., & Perona, P. (2003). Visual identification by signature tracking. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *25*(2), 200–217. https://doi.org/10.1109/TPAMI.2003.1177152

Nabeshima, S., Yamamoto, S., Agusa, K., & Taguchi, T. (1995). MEMO-PEN. In *Conference companion on Human factors in computing systems - CHI '95* (pp.

256–257). New York, New York, USA: ACM Press. https://doi.org/10.1145/223355.223662

Nakanishi, I., Nishiguchi, N., Itoh, Y., & Fukui, Y. (2005). On-line signature verification based on subband decomposition by DWT and adaptive signal processing. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, *88*(6), 1–11. https://doi.org/10.1002/ecjc.20143

Nan Li. (2010). Research on Diffie-Hellman key exchange protocol. In *2010 2nd International Conference on Computer Engineering and Technology* (pp. V4-634-V4-637). IEEE. https://doi.org/10.1109/ICCET.2010.5485276

Nanhe, A. M., Kunjir, M. P., Sakdeo, S. V, Tech, B., & Sci, C. (2008). Improved Synonym Approach to Linguistic Steganography " Design and Proof-of-Concept Implementation. Retrieved from https://pdfs.semanticscholar.org/3dc7/114f2207a5af8feb4e1321383558a3ce83da.pdf?_ga=2.79591892.1932548700.1523186382-650455174.1523186382

Natalie Wolchover. (2015). A Tricky Path to Quantum-Safe Encryption | News | Communications of the ACM. Retrieved April 8, 2018, from https://cacm.acm.org/news/191786-a-tricky-path-to-quantum-safe-encryption/fulltext

Nechta, I., & Fionov, A. (2011). Applying statistical methods to text steganography. Retrieved from http://arxiv.org/abs/1110.2654

Nel, E.-M., du Preez, J. A., & Herbst, B. M. (2005). Estimating the pen trajectories of static signatures using hidden Markov models. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *27*(11), 1733–1746. https://doi.org/10.1109/TPAMI.2005.221

Nelson, D. A., & Bilger, R. C. (1974). Pure-tone octave masking in normal-hearing listeners. *Journal of Speech and Hearing Research*, *17*(2), 223–251. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/4836042

NELSON, W., TURIN, W., & HASTIE, T. (1994). STATISTICAL METHODS FOR ON-LINE SIGNATURE VERIFICATION. *International Journal of Pattern Recognition and Artificial Intelligence*, *8*(3), 749–770. https://doi.org/10.1142/S0218001494000395

Nguyen-Tan, K., & Nguyen-Hoang, N. (2013). Handwriting Recognition Using B-Spline Curve (pp. 335–346). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-36642-0_33

Nissar, A., & Mir, A. H. (2010). Classification of steganalysis techniques: A study. *Digital Signal Processing*, *20*(6), 1758–1770. https://doi.org/10.1016/J.DSP.2010.02.003

Nosrati, M., Karimi, R., & Hariri, M. (2012). Audio Steganography: A Survey on Recent Approaches. *World Applied Programming*, (23), 202–205. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=E38B5EE9F643592DFFC1C21C593EC0ED?doi=10.1.1.685.2785&rep=rep1&type=pdf

Odeh, A., Alzubi, A., Hani, Q. B., & Elleithy, K. (2012). Steganography by multipoint Arabic letters. In *2012 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1–7). IEEE. https://doi.org/10.1109/LISAT.2012.6223209

Ohishi, T., Komiya, Y., Morita, H., & Matsumoto, T. (n.d.). Pen-input on-line signature verification with position, pressure, inclination trajectories. In *Proceedings 15th International Parallel and Distributed Processing Symposium. IPDPS 2001* (pp. 1757–1763). IEEE Comput. Soc. https://doi.org/10.1109/IPDPS.2001.925164

Ortega-Garcia, J., Fierrez-Aguilar, J., Martin-Rello, J., & Gonzalez-Rodriguez, J. (2003). Complete Signal Modeling and Score Normalization for Function-Based Dynamic Signature Verification (pp. 658–667). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44887-X_77

Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., … Moro, Q.-I. (2003). MCYT baseline corpus: a bimodal biometric database. *IEE Proceedings - Vision, Image, and Signal Processing*, *150*(6), 395. https://doi.org/10.1049/ip-vis:20031078

Ozer, H., Avcibas, I., Sankur, B., & Memon, N. D. (2003). <title>Steganalysis of audio based on audio quality metrics</title> In E. J. Delp III & P. W. Wong (Eds.) (Vol. 5020, pp. 55–66). International Society for Optics and Photonics. https://doi.org/10.1117/12.477313

Özer, H., Sankur, B., Memon, N., & Avcıbaş, İ. (2006). Detection of audio covert channels using statistical footprints of hidden messages. *Digital Signal Processing*, *16*(4), 389–401. https://doi.org/10.1016/J.DSP.2005.12.001

Paone, J., & Flynn, P. J. (2011). On the consistency of the biometric menagerie for irises and iris matchers. In *2011 IEEE International Workshop on Information Forensics and Security* (pp. 1–6). IEEE. https://doi.org/10.1109/WIFS.2011.6123158

Patsakis, C. (2012). Steganalysis of Statistical Restored Stegoimages with Compressive Sensing. In *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 498–501). IEEE. https://doi.org/10.1109/IIH-MSP.2012.126

Percival, D. B., & Mofjeld, H. O. (n.d.). Analysis of Subtidal Coastal Sea Level Fluctuations Using Wavelets. Retrieved from https://pdfs.semanticscholar.org/8d3a/ad5c87dedf2d7dac854d6de6e6dbeb093dfa.pdf

Percival, D. B., & Walden, A. T. (2000). *Wavelet methods for time series analysis*. Cambridge University Press.

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, *87*(7), 1062–1078. https://doi.org/10.1109/5.771065

Pevn, T., & Fridrich, J. (2007). Merging Markov and DCT Features for Multi-Class JPEG Steganalysis. Retrieved from https://pdfs.semanticscholar.org/a7b6/d6089d247a06b6c1c920e76a83d8bf9a3bbf.pdf

Plamondon, R., & Lorette, G. (1989). Automatic signature verification and writer identification — the state of the art. *Pattern Recognition*, *22*(2), 107–131. https://doi.org/10.1016/0031-3203(89)90059-9

Poh, N., & Kittler, J. (2009). A Biometric Menagerie Index for Characterising Template/Model-Specific Variation (pp. 816–827). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-01793-3_83

Poh, N., Thian, H., Marcel, S., & Bengio, S. (n.d.). IMPROVING FACE AUTHENTICATION USING VIRTUAL SAMPLES. Retrieved from http://publications.idiap.ch/downloads/reports/2003/norman_2003_icassp.pdf

Popa, R., S. Tanenbaum, A., Jurca, I., & Hänle, C. (1998). An Analysis of Steganographic Techniques Scientific advisers: Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.88.9413

Popescu-Bodorin, N., Balas, V. E., & Motoc, I. M. (2013). The Biometric Menagerie – A Fuzzy and Inconsistent Concept (pp. 27–43). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33941-7_6

Por, L. Y., & Delina, B. (2008). Information Hiding: A New Approach in Text Steganography. Retrieved from http://www.wseas.us/e-library/conferences/2008/hangzhou/acacos/116-586-634.pdf

Porwik, P., & Lisowska, A. (n.d.). The Haar–Wavelet Transform in Digital Image Processing: Its Status and Achievements. Retrieved from https://pdfs.semanticscholar.org/9b20/ddd6e8b08681a916b7b74b24994bcef31626.pdf

Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. *IEEE Security & Privacy Magazine*, *1*(3), 32–44. https://doi.org/10.1109/MSECP.2003.1203220

Qi, Y., Wang, Y., & Yuan, J. (2009). Audio Steganalysis Based on Co-occurrence Matrix and PCA. In *2009 International Conference on Measuring Technology and Mechatronics Automation* (pp. 433–436). IEEE. https://doi.org/10.1109/ICMTMA.2009.342

Qiao, M., Sung, A. H., & Liu, Q. (2013). MP3 audio steganalysis. *Information Sciences*, *231*, 123–134. https://doi.org/10.1016/J.INS.2012.10.013

Qingzhong Liu, Sung, A. H., Jianyun Xu, & Ribeiro, B. M. (2006). Image Complexity and Feature Extraction for Steganalysis of LSB Matching Steganography. In *18th International Conference on Pattern Recognition (ICPR'06)* (pp. 267–270). IEEE. https://doi.org/10.1109/ICPR.2006.684

Quan, Z.-H., & Liu, K.-H. (2007). Online Signature Verification Based on the Hybrid HMM/ANN Model. *IJCSNS International Journal of Computer Science and Network Security*, *7*(3). Retrieved from https://pdfs.semanticscholar.org/9f1b/adb50408608c565f8f7d8d72ad4de1f02cad.pdf

R, R. H., & S, A. H. (2011). INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY. *The International Journal of Multimedia & Its Applications (IJMA)*, *3*(3). https://doi.org/10.5121/ijma.2011.3308

Rabah, K. (2004). Steganography-The Art of Hiding Data. *Information Technology Journal*, *3*(3), 245–269. https://doi.org/10.3923/itj.2004.245.269

Rabasse, C., Guest, R., & Fairhurst, M. (2007). A Method for the Synthesis of Dynamic Biometric Signature Data. In *Ninth International Conference on Document Analysis and Recognition (ICDAR 2007)* (pp. 168–172). IEEE. https://doi.org/10.1109/ICDAR.2007.4378697

Rabasse, C., Guest, R. M., & Fairhurst, M. C. (2008). A New Method for the Synthesis of Signature Data With Natural Variability. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *38*(3), 691–699. https://doi.org/10.1109/TSMCB.2008.918575

Rajasri, K., & Tindhumathi. (2014). JPEG steganalysis with high-dimensional features and accuracy. In *Proceedings of IEEE International Conference on Computer Communication and Systems ICCCS14* (pp. 010–017). IEEE. https://doi.org/10.1109/ICCCS.2014.7068159

Rashidi, S., Fallah, A., & Towhidkhah, F. (2012). Feature extraction based DCT on dynamic signature verification. *Scientia Iranica*, *19*(6), 1810–1819. https://doi.org/10.1016/J.SCIENT.2012.05.007

Rekik, S., Guerchi, D., Ae, D. A., Hamam, H., & Selouani, S.-A. (2008). Audio Steganography Coding Using the Discrete Wavelet Transforms. *International Journal of Computer Science and Security*, (61), 2012–2079. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.224.4317&rep=rep1&type=pdf

Ross, A., Rattani, A., & Tistarelli, M. (2009). Exploiting the "doddington zoo" effect in biometric fusion. In *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems* (pp. 1–7). IEEE. https://doi.org/10.1109/BTAS.2009.5339011

Rupanshi, & Preeti, V. (2014). Audio Steganography by Direct Sequence Spread Spectrum. *International Journal of Computer Trends and Technology*, *13*(2). Retrieved from http://www.ijcttjournal.org

S, H., Acharya, U. D., A, R., & Kamath, P. R. (2013). A Secure And High Capacity Image Steganography Technique. https://doi.org/10.5121/sipij.2013.4108

Saha, B., Sharma, S., & Sharma, S. (2012). Steganographic Techniques of Data Hiding Using Digital Images (Review Paper). *Defence Science Journal*, *62*(1), 11–18. https://doi.org/10.14429/dsj.62.1436

Sallee, P. (2004). Model-Based Steganography (pp. 154–167). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24624-4_12

Salomon, D. (2003). Data Hiding in Text. In *Data Privacy and Security* (pp. 245–267). New York, NY: Springer New York. https://doi.org/10.1007/978-0-387-21707-9_11

Saper, N. (2013). International Cryptography Regulation and the Global Information Economy International Cryptography Regulation and the Global Information Economy International Cryptography Regulation and the Global Information Economy. *Northwestern Journal of Technology and Intellectual Property J. Tech. & Intell. Prop*, *11*(7). Retrieved from http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss7/5

Sardha Wijesoma, W., Mingming, M., & Yue, K. W. (2001). On-Line Signature Verification Using a Computational Intelligence Approach (pp. 699–711). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45493-4_69

Sarkar, A. (2010). *Novel Image Data-Hiding Methodologies for Robust and Secure Steganography with Extensions to Image Forensics | Vision Research Lab*. University of California, Santa Barbara. Retrieved from https://vision.ece.ucsb.edu/sites/vision.ece.ucsb.edu/files/publications/Anindya-thesis.pdf

saroha, kriti, & Singh, D. P. K. (2009). A survey on text based steganography. *Proceedings*. Retrieved from http://www.academia.edu/2082567/A_Survey_on_Text_Based_Steganography

Sencar, H. T. (2006). Performance study of common image steganography and steganalysis techniques. *Journal of Electronic Imaging*, *15*(4), 41104. https://doi.org/10.1117/1.2400672

Shafiei, M. M., & Rabiee, H. R. (2003). A new online signature verification algorithm using variable length segmentation and hidden Markov models. In *Seventh International Conference on Document Analysis and Recognition, 2003. Proceedings.* (Vol. 1, pp. 443–446). Edinburgh, UK: IEEE Comput. Soc. https://doi.org/10.1109/ICDAR.2003.1227706

Shah, V., Sanghavi, U., & Shah, U. (2013). Off-line signature verification using curve fitting algorithm with neural networks. In *2013 International Conference on Advances in Technology and Engineering (ICATE)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICAdTE.2013.6524770

Shakil, A., Ahmad, S. M. S., Anwar, R. B. M., & Balbed, M. A. M. (2008). Analysis of the Effect of Different Features' Performance on Hidden Markov Modeling Based Online and Offline Signature Verification Systems. In *2008 Digital Image Computing: Techniques and Applications* (pp. 572–577). IEEE. https://doi.org/10.1109/DICTA.2008.76

Shamim Mohammad Arif, A., Sabbir Hussain, M., Rafiqul Islam, M., Ahsan Rajon, S. A., & Al Nahid, A. (n.d.). AN APPROACH FOR OFF-LINE SIGNATURE VERIFICATION SYSTEM USING PEAK AND CURVE COMPARISON. Retrieved from http://ijcit.org/jcit_papers/vol-1_no-1/JCIT-100706.pdf

Sharma, M., & Swagota Bera, M. (2012). A REVIEW ON BLIND STILL IMAGE STEGANALYSIS TECHNIQUES USING FEATURES EXTRACTION AND PATTERN CLASSIFICATION METHOD. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, *2*(3). https://doi.org/10.5121/ijcseit.2012.2308

Sharma, S., Yadav, V. K., & Batham, S. (2014). Zero Distortion Technique: An Approach to Image Steganography Using Strength of Indexed Based Chaotic Sequence (pp. 407–416). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44966-0_40

Sheikhan, M., Moin, M. S., & Pezhmanpour, M. (2010). Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform. In *2010 10th International Conference on Intelligent Systems Design and Applications* (pp. 368–372). IEEE. https://doi.org/10.1109/ISDA.2010.5687236

Sheskin, D. (2011). *Handbook of parametric and nonparametric statistical procedures*. Chapman & Hall/CRC.

Shimizu, H., Kiyono, S., Motoki, T., & Gao, W. (2004). An electrical pen for signature verification using a two-dimensional optical angle sensor. *Sensors and Actuators A: Physical*, *111*(2–3), 216–221. https://doi.org/10.1016/J.SNA.2003.11.014

Shirali-Shahreza, M. (2007). Improving Mobile Banking Security Using Steganography. In *Fourth International Conference on Information Technology (ITNG'07)* (pp. 885–887). IEEE. https://doi.org/10.1109/ITNG.2007.108

Shirali-Shahreza, M. (2008). Text Steganography by Changing Words Spelling. In *2008 10th International Conference on Advanced Communication Technology* (pp. 1912–1913). IEEE. https://doi.org/10.1109/ICACT.2008.4494159

Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2006). A New Approach to Persian/Arabic Text Steganography. In *5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering,Software Architecture and Reuse (ICIS-COMSAR'06)* (pp. 310–315). IEEE. https://doi.org/10.1109/ICIS-COMSAR.2006.10

Shirali-Shahreza, S., & Manzuri-Shalmani, M. T. (2008). High capacity error free wavelet Domain Speech Steganography. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 1729–1732). IEEE. https://doi.org/10.1109/ICASSP.2008.4517963

Shirali-Shahreza, S., & Shirali-Shahreza, M. (2008). Steganography in Silence Intervals of Speech. In *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 605–607). IEEE. https://doi.org/10.1109/IIH-MSP.2008.5

Shiva Kumar, K. B., Raja, K. B., Chhotaray, R. K., & Pattnaik, S. (2011). Steganography Based on Payload Transformation. *IJCSI International Journal of Computer Science Issues ISSN*, *8*(2), 1694–1814. Retrieved from

Shivani, Yadav, V. K., & Batham, S. (2014). Zero Distortion Technique. In *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '14* (pp. 1–8). New York, New York, USA: ACM Press. https://doi.org/10.1145/2677855.2677905

Shivani, Yadav, V. K., & Batham, S. (2015). A Novel Approach of Bulk Data Hiding using Text Steganography. *Procedia Computer Science*, *57*, 1401–1410. https://doi.org/10.1016/J.PROCS.2015.07.457

Shunquan Tan, & Bin Li. (2012). Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting. *IEEE Signal Processing Letters*, *19*(6), 336–339. https://doi.org/10.1109/LSP.2012.2194702

Simmons, G. J. (1984). The Prisoners' Problem and the Subliminal Channel. In *Advances in Cryptology* (pp. 51–67). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4684-4730-9_5

Siyuan Chen, & Srihari, S. (2005). Use of exterior contours and shape features in off-line signature verification. In *Eighth International Conference on Document Analysis and Recognition (ICDAR'05)* (p. 1280–1284 Vol. 2). IEEE. https://doi.org/10.1109/ICDAR.2005.249

Stanković, R. S., & Falkowski, B. J. (2003). The Haar wavelet transform: its status and achievements. *Computers & Electrical Engineering*, *29*(1), 25–44. https://doi.org/10.1016/S0045-7906(01)00011-8

Stojanov, I., Mileva, A., & Stojanovic, I. (2014). A New Property Coding in Text Steganography of Microsoft Word Documents. Retrieved from http://eprints.ugd.edu.mk/11385/

Subhedar, M. S., & Mankar, V. H. (2014). Current status and key issues in image steganography: A survey. *Computer Science Review*, *13–14*, 95–113. https://doi.org/10.1016/J.COSREV.2014.09.001

Sumathi, C. P., Santanam, T., & Umamaheswari, G. (2014). A Study of Various Steganographic Techniques Used for Information Hiding. Retrieved from http://arxiv.org/abs/1401.5561

Sun, Z., Hui, M., & Guan, C. (2008). Steganalysis Based on Co-occurrence Matrix of Differential Image. In *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 1097–1100). IEEE.

https://doi.org/10.1109/IIH-MSP.2008.176

Swanson, M. D., Kobayashi, M., & Tewfik, A. H. (1998). Multimedia Data-Embedding and Watermarking Technologies. Retrieved from https://pdfs.semanticscholar.org/e177/2e96e51dc39c8966bda77c11ea29c784b27a.pdf

Syed Ahmad, S. M., Shakil, A., Ahmad, A. R., Muhamad Balbed, M. A., & Anwar, R. M. (2008). SIGMA - A Malaysian signatures' database. In *2008 IEEE/ACS International Conference on Computer Systems and Applications* (pp. 919–920). IEEE. https://doi.org/10.1109/AICCSA.2008.4493644

Syed Ahmad, S. M., Shakil, A., Ahmad Faudzi, M., & Anwar, R. M. (2010). Analysis of "goat" within user population of an offline signature biometrics. In *10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010)* (pp. 765–769). IEEE. https://doi.org/10.1109/ISSPA.2010.5605415

Tan, K. T., Ghanbari, M., & Pearson, D. E. (1998). An objective measurement tool for MPEG video quality. *Signal Processing*, *70*(3), 279–294. https://doi.org/10.1016/S0165-1684(98)00129-7

Taskiran, C. M., Topkara, U., Topkara, M., & Delp, E. J. (2006). Attacks on lexical natural language steganography systems. In E. J. Delp III & P. W. Wong (Eds.) (p. 607209). https://doi.org/10.1117/12.649551

Tong Qu, Abdulmotaleb El Saddik, & Adler, A. (n.d.). Dynamic signature verification system using stroked based features. In *The 2nd IEEE Internatioal Workshop on Haptic, Audio and Visual Environments and Their Applications, 2003. HAVE 2003. Proceedings.* (pp. 83–88). IEEE. https://doi.org/10.1109/HAVE.2003.1244730

Tzschoppe, R., Bäuml, R., Huber, J. B., & Kaup, A. (2003). Steganographic System Based on Higher-Order Statistics. *Proceedings of SPIE*, *5020*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.5800&rep=rep1&type=pdf

Vargas, F., Ferrer, M., Travieso, C., & Alonso, J. (2007). Off-line Handwritten Signature GPDS-960 Corpus. In *Ninth International Conference on Document Analysis and Recognition (ICDAR 2007) Vol 2* (pp. 764–768). IEEE. https://doi.org/10.1109/ICDAR.2007.4377018

Vargas, J. F., Ferrer, M. A., Travieso, C. M., & Alonso, J. B. (2011). Off-line signature verification based on grey level information using texture features. *Pattern Recognition*, *44*(2), 375–385. https://doi.org/10.1016/J.PATCOG.2010.07.028

Viard-Gaudin, C., Lallican, P. M., Knerr, S., & Binter, P. (1999). The IRESTE On/Off (IRONOFF) dual handwriting database. In *Proceedings of the Fifth International Conference on Document Analysis and Recognition. ICDAR '99 (Cat. No.PR00318)* (pp. 455–458). IEEE. https://doi.org/10.1109/ICDAR.1999.791823

Vibha, M., & Sanjivani Shantaiya, P. M. (2012). Signature Verification Using Morphological Features Based on Artificial Neural Network. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(7), 2277–128. Retrieved from https://pdfs.semanticscholar.org/5ff9/662db2f33df59e8b70a2237358bee74c1849.pdf

Viriri, S. (2014). Handwritten Signature Verification Based on Enhanced Direction and Grid Features (pp. 820–829). Springer, Cham. https://doi.org/10.1007/978-3-319-14364-4_79

Walden, A. T., & Cristan, A. C. (1998). The phase-corrected undecimated discrete wavelet packet transform and its application to interpreting the timing of events. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *454*(1976), 2243–2266. https://doi.org/10.1098/rspa.1998.0257

Wang, H., & Wang, S. (2004). Cyber warfare. *Communications of the ACM*, *47*(10), 76–82. https://doi.org/10.1145/1022594.1022597

Wang, Y., & Moulin, P. (2007). Optimized Feature Extraction for Learning-Based Image Steganalysis. *IEEE Transactions on Information Forensics and Security*, *2*(1), 31–45. https://doi.org/10.1109/TIFS.2006.890517

Wang, Z., Sheikh, H. R., & Bovik, A. C. (2003). OBJECTIVE VIDEO QUALITY ASSESSMENT, 1041–1078. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.79.2528&rep=rep1&type=pdf

Watters, P. A., Martin, F., & Stripf, H. S. (n.d.). Visual Steganalysis of LSB-Encoded Natural Images. In *Third International Conference on Information Technology and Applications (ICITA'05)* (Vol. 1, pp. 746–751). IEEE. https://doi.org/10.1109/ICITA.2005.308

Wei Zeng, Haojun Ai, & Ruimin Hu. (2008). An algorithm of echo steganalysis based on power cepstrum and pattern classification. In *2008 International Conference on Audio, Language and Image Processing* (pp. 1344–1348). IEEE. https://doi.org/10.1109/ICALIP.2008.4590036

Wessels, T., & Omlin, C. W. (2000). A hybrid system for signature verification. In *Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. IJCNN 2000. Neural Computing: New Challenges and Perspectives for the New Millennium* (pp. 509–514 vol.5). IEEE. https://doi.org/10.1109/IJCNN.2000.861520

Westfeld, A. (2003). Detecting Low Embedding Rates. In *International Workshop on Information Hiding* (pp. 324–339). Springer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.138.8578&rep=rep1&type=pdf

Westfeld, A., & Pfitzmann, A. (2000). Attacks on Steganographic Systems (pp. 61–76). Springer, Berlin, Heidelberg. https://doi.org/10.1007/10719724_5

Wirotius, M., Ramel, J.-Y., & Vincent, N. (2004). Selection of Points for On-Line Signature Comparison. In *Ninth International Workshop on Frontiers in Handwriting Recognition* (pp. 503–508). IEEE. https://doi.org/10.1109/IWFHR.2004.92

Wittman, M., Davis, P., & Flynn, P. J. (n.d.). Empirical Studies of the Existence of the Biometric Menagerie in the FRGC 2.0 Color Image Corpus. In *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)* (pp. 33–33). IEEE. https://doi.org/10.1109/CVPRW.2006.71

Wu, H. R. (Hong R., & Rao, K. R. (Kamisetty R. (2006). *Digital video image quality and perceptual coding*. CRC/Taylor & Francis.

Wu, S. X., & Banzhaf, W. (2010). A hierarchical cooperative evolutionary algorithm. In *Proceedings of the 12th annual conference on Genetic and evolutionary computation - GECCO '10* (p. 233). New York, New York, USA: ACM Press. https://doi.org/10.1145/1830483.1830527

Xiang, L., Sun, X., Luo, G., & Gan, C. (2007). Research on Steganalysis for Text Steganography Based on Font Format. In *Third International Symposium on Information Assurance and Security* (pp. 490–495). IEEE. https://doi.org/10.1109/IAS.2007.48

Xiao, X.-H., & Leedham, G. (n.d.). Signature Verification by Neural Networks with Selective Attention. *Applied Intelligence*, *11*(2), 213–223. https://doi.org/10.1023/a:1008380515294

Xiao, X., Preneel, B., Preneel, B., Foresti, S., Kirda, E., Katzenbeisser, S., … Yang, B.-Y. (2011). Man-in-the-Middle Attack. In *Encyclopedia of Cryptography and Security* (pp. 759–759). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-5906-5_324

Xiaoxiao Dong, Bocko, M. F., & Ignjatovic, Z. (2004). Data hiding via phase manipulation of audio signals. In *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing* (Vol. 5, p. V-377-80). IEEE. https://doi.org/10.1109/ICASSP.2004.1327126

Xiaoyi Jiang, Bunke, H., Abegglen, K., & Kandel, A. (n.d.). Curve morphing by weighted mean of strings. In *Object recognition supported by user interaction for service robots* (Vol. 4, pp. 192–195). IEEE Comput. Soc. https://doi.org/10.1109/ICPR.2002.1047430

Xiaoyi Yu, Yunhong Wang, & Tieniu Tan. (2004). On estimation of secret message length in JSteg-like steganography. In *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.* (p. 673–676 Vol.4). IEEE. https://doi.org/10.1109/ICPR.2004.1333862

Xuan, G., Shi, Y. Q., Gao, J., Zou, D., Yang, C., Zhang, Z., … Chen, W. (2005). Steganalysis Based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions (pp. 262–277). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11558859_20

Xuanwen Luo, Qiang Cheng, & Tan, J. (2003). A lossless data embedding scheme for medical images in application of e-diagnosis. In *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE Cat. No.03CH37439)* (pp. 852–855). IEEE. https://doi.org/10.1109/IEMBS.2003.1279899

Yager, N., & Dunstone, T. (2007). Worms, Chameleons, Phantoms and Doves: New Additions to the Biometric Menagerie. In *2007 IEEE Workshop on Automatic Identification Advanced Technologies* (pp. 1–6). IEEE. https://doi.org/10.1109/AUTOID.2007.380583

Yager, N., & Dunstone, T. (2010). The Biometric Menagerie. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *32*(2), 220–230. https://doi.org/10.1109/TPAMI.2008.291

Yang, H., & Cao, X. (2010). Linguistic steganalysis based on meta features and immune mechanism. *Chinese Journal of Electronics*, *19*(4), 661–666.

Yavanoglu, U., Ozcakmak, B., & Milletsever, O. (2012). A New Intelligent Steganalysis Method for Waveform Audio Files. In *2012 11th International Conference on Machine Learning and Applications* (pp. 233–239). IEEE. https://doi.org/10.1109/ICMLA.2012.150

Yazid, Ahmad Sanmorino, S. (2012). A survey for handwritten signature verification - Semantic Scholar. In *2nd International Conference on Uncertainty Reasoning*

and Knowledge Engineering. Retrieved from https://www.semanticscholar.org/paper/A-survey-for-handwritten-signature-verification-Sanmorino-Yazid/8a56e5a7aea28487ec71d2ca9c37c8dce6fdaca5

Ye, L., Qi, X.-J., Lv, L.-J., & Zuo, Y. (2012). Time domain speech steganalysis method based on multiplicative embedding model. In *2012 International Conference on Wavelet Analysis and Pattern Recognition* (pp. 148–151). IEEE. https://doi.org/10.1109/ICWAPR.2012.6294769

Yeung, D.-Y., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., & Rigoll, G. (2004). SVC2004: First International Signature Verification Competition (pp. 16–22). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-25948-0_3

Yilmaz, M. B., Yanikoglu, B., Tirkaz, C., & Kholmatov, A. (2011). Offline signature verification using classifier combination of HOG and LBP features. In *2011 International Joint Conference on Biometrics (IJCB)* (pp. 1–7). IEEE. https://doi.org/10.1109/IJCB.2011.6117473

Yu, Z., Huang, L., Chen, Z., Li, L., Zhao, X., & Zhu, Y. (2008). Detection of Synonym-Substitution Modified Articles Using Context Information. In *2008 Second International Conference on Future Generation Communication and Networking* (pp. 134–139). IEEE. https://doi.org/10.1109/FGCN.2008.39

Zamani, M., Manaf, A. A., B. Ahmad, R., M. Zeki, A., & Abdullah, S. (2009). A Genetic-Algorithm-Based Approach for Audio Steganography. *World Academy of Science, Engineering and Technology*, *54*, 360–363. Retrieved from https://waset.org/publications/9304/a-genetic-algorithm-based-approach-for-audio-steganography

Zeng, W., Ai, H., & Hu, R. (2007). A Novel Steganalysis Algorithm of Phase Coding in Audio Signal. In *Sixth International Conference on Advanced Language Processing and Web Information Technology (ALPIT 2007)* (pp. 261–264). IEEE. https://doi.org/10.1109/ALPIT.2007.41

Zhang, J., Cox, I. J., & Doerr, G. (2007). Steganalysis for LSB Matching in Images with High-frequency Noise. In *2007 IEEE 9th Workshop on Multimedia Signal Processing* (pp. 385–388). IEEE. https://doi.org/10.1109/MMSP.2007.4412897

Zhang, T., & Ping, X. (2003). A fast and effective steganalytic technique against JSteg-like algorithms. In *Proceedings of the 2003 ACM symposium on Applied computing - SAC '03* (p. 307). New York, New York, USA: ACM Press. https://doi.org/10.1145/952532.952595

Zhang, Z., Wang, K., & Wang, Y. (2011). A Survey of On-line Signature Verification (pp. 141–149). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25449-9_18

Zhi-Hui Wang, The Duc Kieu, Chin-Chen Chang, & Ming-Chu Li. (2009). Emoticon-based text steganography in chat. In *2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA)* (pp. 457–460). IEEE. https://doi.org/10.1109/PACIIA.2009.5406559

Zhi-li, C., Liu-sheng, H., Zhen-shan, Y., Ling-jun, L., & Wei, Y. (2008). A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words. In *2008 Third International Conference on Availability, Reliability and Security* (pp. 558–563). IEEE. https://doi.org/10.1109/ARES.2008.61

Zou, D., Shi, Y., Su, W., & Xuan, G. (2006). Steganalysis based on Markov Model of Thresholded Prediction-Error Image. In *2006 IEEE International Conference on Multimedia and Expo* (pp. 1365–1368). IEEE. https://doi.org/10.1109/ICME.2006.262792