Hybridity of Cryptography and Steganography Techniques: Current Status

Rana Saad Mohammed[a] , Sattar B. Sadkhan [b]
[a] Computer Science Dept., Education College, Mustansiriyah University,Baghdad, Iraq
Ranasaad2014@gmail.com
[b] Information Technology College, Babylon University, Hilla, Iraq
drengsattar@ieee.org

Abstract. Information Security is considered as an important research field. Steganography and cryptography are important techniques that preserve on the secrecy of sensitive information. This paper presents the current status of a steganography mechanism and their relationship with cryptographic techniques (especially the newest ones like chaos cryptography) under the new trends of multidisciplinary prospective techniques. And also presents the implementation of chaotic maps with steganography techniques.

Keywords: steganography, cryptography, chaos, information hiding.

1 INTRODUCTION

In recent years, the technologies are growth, such that a people prefer the use of wireless communication as a primary channel to transmit a data through the world. That means data security becomes important to protect information from the eavesdropping and modification over the Internet. There are many developed security techniques ; like cryptography, steganography, to protect a data [1].

Both of steganography and cryptography used for concealing information. But the steganography does not detect any doubt about the hidden information that helps the attacker.

Cryptography used to change the form of data. Steganography hides the existence of data itself that cause the attacker cannot find out where a hidden place of message in easy. Both techniques can be combined to get better protection of information [2].

This paper describes a steganography mechanism in section II. Steganography in digital mediums in section III. Benefits of steganography and its drawbacks in section IV. The used performance measures in section V. Chaotic based steganography and their important rule as a hybrid structure combine both crypto and stego techniques give in section VI.

2 STEGANOGRAPHY TECHNIQUES

Steganography techniques based on replacing bits of useless data with bits of important information. There are three methods of steganography: “Pure steganography”, “secret key steganography”, and “public key steganography”.

The “ Pure Steganography ” method does not require any exchange of secret tool between a sender and receiver like the exchange of a stego-key as shown in figure 1. This method offers less secrecy since the sender and receiver communicate over open system like the Internet and they suppose that there is no a third party between of them [3].

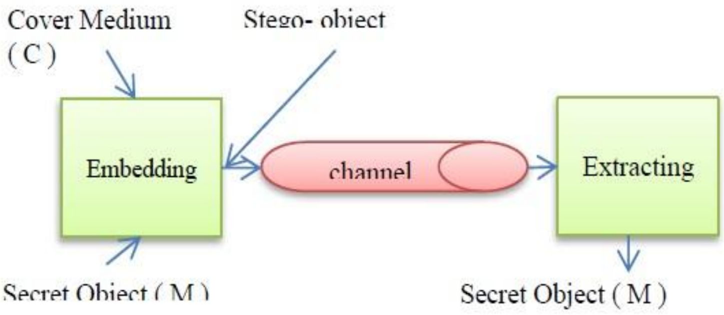

Fig.1. Pure steganography Method

In a " secret key steganography " method, there is a prior secret session for exchanging a stego-key. Then the sender can embed a secret message in a cover which help a secret stego-key to get a stego-object and send it through the internet. The receiver receives a stego-object and extracts a message using an agreed stego-key. The advantage of this method that even if it is intercepted then only authorized parties knows a secret stego-key to extract a secret message.

A general block diagram of steganography is shown in Figure 2 . It contains three basic components:- "original message (M)", "cover medium (C)", and "stego-key" (K) to get a stego-object ($\tilde{\boldsymbol{c}}$) Or embedded message ($\boldsymbol{E_m}$) [4].

$$E_m: C \oplus K \oplus M \rightarrow \tilde{c}$$

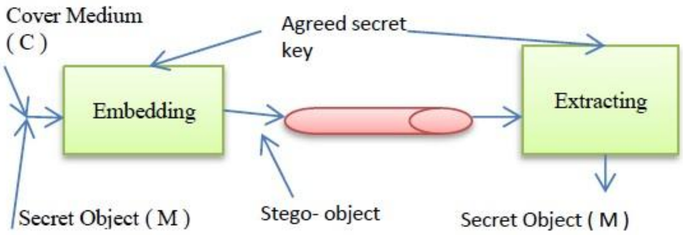

Fig.2. Secret key steganography

To extract the original message from a received stego-object by an authorized receiver. It must have a same key of the sender to get the extracted message ($\boldsymbol{E_x}$).

A cover medium means text, image, audio, or video in which the original secret message will be embedded. An original message also text, images, audio, or video which can be embedded in cover medium to help a stego-key to get a stego message [5].

In " public key steganography" method, it is like a concept of public key cryptography. The sender embeds a secret message in a cover using a public key to get a stego message and send it through the internet. The receiver can extract a secret message using a secret private key. This method is more robust against the attacker since it has multiple levels of security and the attacker requires a time to intercept a secret message as shown in figure 3 .

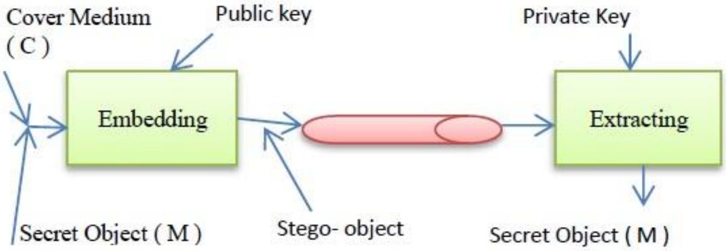

Fig.3. Public key steganography

There are two techniques are related to steganography in closely and have different algorithms to protect a publishing and copyright. These techniques are fingerprinted and watermarking. Fingerprint algorithms embed a unique signature of the publisher in his publishing copies using a specific way of embedding for different publishers. While the algorithms of watermarking embed a mark or signature in the carrier objects using the same embedded method. Signature and marks in the watermarking and fingerprint are hidden using a specific method, although it visible and public knowledge [4][7].

Steganography has widely used in areas like "Military", "Banking", "Market Applications", "Secret Communication", "Copyright Protection", "Feature Tagging", "Digital Watermarking". There are six **attacks against** Steganography algorithms:

- ✓ Stego only attack – only the stego object is available for analysis.
- ✓ Known cover attack – the original cover object and the stego object are available for analysis.
- ✓ Known message attack – the hidden message is available to compare with the stego object.
- ✓ Chosen stego attack – the stego tool (algorithm) and stego-object are available for analysis.
- ✓ Chosen message attack – takes a chosen message and generates a stego object for future analysis.
- ✓ Known stego attack –the stego tool (algorithm), the cover message and the stego-objects are available for analysis [6] .

3 STEGANOGRAPHY IN DIGITAL MEDIUMS

Steganography can use all types of digital file formats for hiding information, in specialist only those have more redundant bits that it necessary to embed secret message bits inside it. The basic types of digital file formats that can be used with steganography are: ("text", "image", "audio", "video", and "protocol") [7].

- Text file format: a secret message can be hidden in each character of the word in a cover text. This method has less used after invention of other different digital file formats. And also a text files have not more redundant data to hide a message.

- Image file format: a secret message can hide in a cover image using a specific algorithm and stego-key to get a stego image. The receiver can extract it from a stego image using a same stego-key at the sender. There are several techniques for image file format:

  - ✓ Spatial domain techniques: “Least Significant Bit, Pseudorandom Permutation, Palette Based Image, Cover Regions and Parity Bits, Quantization and Dithering, Image, Downgrading and cover Channels”.
  - ✓ Masking and filtering.
  - ✓ Transform techniques.
  - ✓ Statistical methods.
  - ✓ Spread Spectrum.
  - ✓ Distortion Techniques.
  - ✓ Cover Generation Techniques.
  - ✓ File and Palette Embedding.

- Audio file format: The examples of digital audio file format are “WAVE”, “MIDI”, “AVI”, “MPEG” or etc.

This technique hides information in cover sound parts that are unnoticeable by human ear.

- Video file format: The examples of digital video format are “H.264”, “Mp4”, “MPEG”, “AVI” or etc. These formats can be used for hiding any kind of secret message.

- Protocol steganography: The protocols (TCP, UDP, ICMP, and IP) are used in information hiding. For example, a secret message is embedded in a header of a protocol packet [8].

4 BENEFITS AND DRAWBACKS OF STEGANOGRAPHY

- STEGANOGRAPHY ADVANTAGES

  - ✓ Steganography can hide the existence of the message such that the attacker cannot guess about where the message is embedded.

  - ✓ It preserves and protects a copyright of publisher copies that contain important information.

  - ✓ It keeps on the secrecy of secret confidential data, such as "credit card numbers", debit cards", and "personal bank accounts".

  - ✓ It provides a secrecy service that encourages a people used it to embed their messages into a cover.

  - ✓ It is interested in publishing and broadcasting industries. To hide an encrypted copyright mark and serial number in "digital films", "audio recording", "books", and "multimedia products" [6].

- STEGANOGRAPHY DRAWBACKS

  - ✓ If its algorithm is intercepted then the attacker can find the place of hidden messages and he can read it. Such drawback can be overcome by combined steganography with cryptography (to strength it by encrypt the message before embedded it).

  - ✓ A hidden message can be destroyed easily. For example, if the secret message embedded in least significant bits of cover. So the interceptor can destroy the message by making a slight change.

  - ✓ Steganography needs an appropriate size of cover medium and redundant data to be can hide a message.

5 PERFORMANCE MEASURES

The performance of steganography algorithms can be measured by comparing between a cover medium and a stego to determine how much the difference between them that gives a powerful to steganography algorithm.

There are statistical measures that help to evaluate the performance, such as: "PSNR (Peak Signal to Noise Ratio)", "MSE (Mean Square Error)", "SNR (Signal to Noise Ratio)", "NCC (Normalized Cross-Correlation)", "BER (Bit Error Rate)".

In addition, steganography algorithms must have robustness against statistical attacks and manipulation transformations such as "linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression.

The algorithms of steganography also must take into account the capacity of secret information with the choice of a suitable cover medium with the use of various types of format to embed such information as invisible to make a process of attack as very complicated task [6][7].

6 CHAOTIC IN STEGANOGRAPHY

In the last decade, chaos theory was developed by physicists and mathematicians. It deals with nonlinear functions. It has desirable features such as "deterministic", "nonlinear", "irregular", "long-term prediction", and "sensitivity to initial conditions".

One of these studies used chaos theory with " Information Security Techniques " like cryptography, steganography to strength the security. These techniques must be evolved with the development of communication technologies.

The chaotic maps that are used in cryptography are: "Logistic map", "Standard map", "Picewise linear chaotic map (PLCM)", "Lorenz map", "Chen map", "Henon map", "Cat map (Arnold map)", "Chebyshev map", "Beta-transformation map" [9]. The security of steganography, by combining it with cryptography [10]. The researchers aimed toward such direction are:

In [11] proposed Chaotic Pixel Value Difference (C-PVD) approach. It used (1D) logistic map or(2D) Arnold cat map in encryption with traditional steganography to get secure payload.

In [12] proposed chaotic pseudo random bit sequence (C-PRBG) to generate a key has size equal to biometric identifies the data as one time pad concept. C-PRBG can generate a sequence of key by mixing three different (1D) chaotic maps as follows:

$$k(i) = \begin{cases} 1 & F_3(x_1(i), p_3) > F_3(x_2(i), p_3) \\ k(i-1) & F_3(x_1(i), p_3) = F_3(x_2(i), p_3) \\ 0 & F_3(x_1(i), p_3) < F_3(x_2(i), p_3) \end{cases} \tag{1}$$

Where p_1, p_2 and p3 are control parameters, $x_1(0)$, $x_2(0)$ and $x_3(0)$ are initial conditions and x1(i), x2(i), x3(i) denote the three chaotic orbits. The next values of chaotic orbits x_1, x_2, and x_3 as follows:

$$\begin{aligned} x_1(i+1) &= F_1(x_1(i), p_1) \\ x_2(i+1) &= F_2(x_2(i), p_2) \\ x_3(i+1) &= F_3(x_3(i), p_3) \end{aligned} \tag{2}$$

Where $F_1(x_1; p_1)$, $F_2(x_2; p_2)$ and $F_3(x_3; p_3)$ are three different (1D) chaotic maps.

In [10] used Indexed Based Chaotic Sequence for encryption purpose by using (Logistic map). There other researchers used this technique existing in [13][14]. In [15] used Peace Wise Linear Chaotic Map (PWLCM) to enhance LSB-DCT technique. PWLCM used to generate a series that helps for randomly embedding of secret image in the DCT coefficients of cover image.

In [16] proposed (3D) chaotic map to develop a spatial steganography method by embed secret message into a cover image randomly. The equation of use (3D) chaotic map as follows:

$$\begin{aligned} x_{n+1} &\equiv \left[\frac{1}{\alpha_1^2 y_n z_n} tan^2\left(arctan\left(\sqrt{x_n}\right)\right)\right] \; mod\; 1 \\ y_{n+1} &\equiv \left[\frac{1}{\alpha_2^2 x_n z_n} sin^2\left(arctan\left(\frac{1}{\sqrt{y_n}}\right)\right)\right] \; mod\; 1 \\ z_{n+1} &\equiv \left[\frac{1}{\alpha_3^2 x_n y_n} \left|tan\left(arctan(|z_n|)\right)\right|\right] \; mod\; 1 \end{aligned} \tag{3}$$

In [17] used an Arnold map to scramble a secret image with key. This method applied fractional Fourier transform and then applied DWT to both of cover and secret images. Then the addition process can be applied using alpha blending technique between the DWT coefficients of cover and secret images.

In [18] used logistic chaotic map for encrypting a secret text and for embedding in DCT cover image. In [19] used Henon chaotic map to scramble a secret image and then embed the result in cover image coefficients of 2D DWT.

In [20] messages embedded in LSB image randomly using subsection linear chaotic map according to the perturbing algorithm presented in [21]:

$$f(x) = \begin{cases} g(x) & x \notin c_3 \\ g\left(\frac{4}{2\varepsilon}(x-0.5)\right) & x \in c_{31} \\ g\left(\frac{x-\left(0.5+\frac{\varepsilon}{4}\right)}{1-\varepsilon} + 0.75\right) & x \in c_{31} \end{cases} \tag{4}$$

Where consider a (1D) subsection linear chaotic mapping with four subintervals:

$$g(x) = \begin{cases} 4x & 0 \le x < a \\ 2-4x & a \le x < b \\ 4x-2 & b \le x < 1-a \\ -4x & 1-a \le x \le 1 \end{cases} \tag{5}$$

By diffuse a third subinterval as c3 = [b, 1 − a): “divide c3 into two segments according to e : 1 − e scale: c31 = [b, b + e/r) and c32 = [b + e/r, 1 − a], where (e) is diffused coefficient, r is constant, x is initial number”. Let a = 0.25, b = 0.5 and r = 4, then obtain a subsection linear chaotic mapping according to the perturbing algorithm as equation (4).

7 CONCLUSION

Steganography is an information hiding technique. There is more research tries to strength it. From one point steganography can be combined with cryptography to increase its security. Modern researches oriented their aims toward using chaotic maps in steganography to improve the overall security aspects of the whole resulted Hybrid Security System, and also to increase the cryptanalytic efforts that must be paid to cryptanalysis the complete hybrid (Crypto- Stego) system . The performance results of such hybrid systems are acceptable. And the use of different chaotic maps is recommended in the future works.

Acknowledgments

We would like to express our sincere gratitude and thanks to the organization committee of ICCIIDT 2016 conference and in a specialist to a Professor Dr. Ibrahim El-Emary, Ph.D. of computer science and systems, University of king Abdul Aziz, KSA for his continuous support, cooperation, and assistance.

References

[1] Majumder, J., & Mangal, S. (2012). An Overview of Image Steganography using LSB Technique. IJCA Proceedings on National Conference on Advances in Computer Science and Applications (NCACSA 2012) NCACSA(3).

[2] Poornima, R., & Iswarya, R.J. (2013). Overview of Digital Image Steganography. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1.

[3] Ashok, J., Raju, Y., Munishankaraiah, S., & Srinivas, K. (2010). Steganography: An Overview. International Journal of Engineering Science and Technology Vol. 2(10).

[4] Kamdar, N. P., Kamdar, D.G., & Khandhar, D.N. (2013). Performance Evaluation of LSB based Steganograhy for Optimization of PSNR and MSE. Journal of Information, Knowledge and Research in Electronics and Communication Engineering, vol. 2, no. 2.

[5] Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image Steganography Techniques: An Overview. International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3). p168-187.

[6] Chugh, G. (2013). Image steganography techniques: A review article. ACTA TECHNICA CORVINIENSIS-Bulletin of Engineering. Tome VI (2013) -FASCICULE3 [JULY-SEPTEMBER]. ISSN 2067-3809. P. 97-104.

[7] Morkel, T. , Eloff, J.H.P., & Olivier, M.S. (2005). An Overview of Image Steganography. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[8] Mandal, P. C. (2012). Modern Steganographic technique: A survey. International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345 Vol. 3 No. 9.

[9] Mohammed, R. S., & Sadkhan, S.B. (2014). Chaos-Based Cryptography for Voice Secure Wireless Communication", pp 97-126 as a chapter 4 of book "Multidisciplinary Perspectives in Cryptology and Information Security". IGI Global. USA.

[10] Shivania, Kumar, V., & Bathamb, Y.S. (2015). A Novel Approach of Bulk Data Hiding using Text Steganography. Procedia Computer Science, 57, 1401 – 1410.

[11] Pun, N., & Juneja, M. (2016). Chaotic Pixel Value Differencing. Copyright © 2016 MECS I.J. Image, Graphics and Signal Processing, 4, 54-60.

[12] Ntalianis, K., & Tsapatsoulis, N. (2016). Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks. IEEE transaction on EMERGING TOPICS IN COMPUTING. V. 4, NO. 1. P 156-174.

[13] Batham, S., Acharya, A., Yadav, V.K., & Paul, R. (2013). A New Video Encryption Algorithm Based on Indexed Based Chaotic Sequence.CONFLUENCE-2013, IET digital library.http://digital library.theiet.org/content/conferences/10.1049/cp.2013.2307

[14] Soni, A., & Acharya, A.k. (2012). A Novel Image Encryption Approach Using An Index Based Chaos And DNA Encoding and Its Performance Analysis. IJCA (0975-8887) Volume 47-No. 23, June 2012.

[15] Habib, M., Bakhache, B., Battikh, D., & El Assad, S. (2015). Enhancement using chaos of a Steganography method in DCT domain. IEEE. Digital Information and Communication Technology and its Applications (DICTAP). Fifth International Conference on. P 204 – 209.

[16] Valandar, M.Y. ,Ayubi, P., & Barani, M.J. (2015). High Secure Digital Image Steganography Based On 3D Chaotic Map. International Conference on Information and Knowledge Technology. IEEE.

[17] Garg, S., & Mathur, M. (2014). Chaotic Map Based Steganography of Gray Scale Images in Wavelet Domain. IEEE. International Conference on Signal Processing and Integrated Networks (SPIN). P 689-694.

[18] Saeed, M.J. (2013). A New Technique based on Chaotic Steganography and Encryption Text in DCT Domain for Color Image. Journal of Engineering Science and Technology Vol. 8, No. 5. 508 – 520. School of Engineering, Taylor's University.

[19] Thenmozhi, S. & Chandrasekaran, M. (2013). A Novel Technique for Image Steganography Using Nonlinear Chaotic Map. Proceedings of 7th International Conference on Intelligent Systems and Control. IEEE. P 307-311.

[20] Luo, X., Liu, F., & Lu, P. (2007). A LSB Steganography Approach against Pixels Sample Pairs Steganalysis. International Journal of Innovative Computing, Information and Control ICIC International, ISSN 1349-4198. Volume 3, Number 3. pp. 575—588.

[21] Liu, B., Luo X. & Liu F. (2006). Perturbing scheme of digital chaos, Journal of Shanghai Jiaotong University (Science), English version, vol.11, no.2, pp.172-176, 2006.

Biographies

Rana Saad Mohammed is a lecturer in the computer science department at the College of Education of the University of Mustansiriyah. She received the B.Sc. in computer science from Mustansiriyah University, Baghdad, Iraq in 2006, M.Sc. in computer science from University of Technology ,Baghdad, Iraq in 2008, and Ph.D. in computer science from Babylon University, Hilla, Iraq in 2015.. Her main research interests in Information security, stream cipher, block cipher, pseudorandom number generator, voice encryption, chaos theory, steganography, data mining privacy, Security of Internet of things (IoT), and Cloud computing.

Sattar B. Sadkhan is a professor at the College of Information Technology of the University of Babylon, Hilla, Iraq. He received a PhD degree in Wireless Communication Engineering in 1984, and MSc degree from the VAAZ Academy in Brno, Czech Republic in 1981. His

BSc degree in Electrical and Electronic Engineering from Military Engineering College (MTC) in Baghdad, Iraq in 1978. He received a Diploma in Radar Repairing (1970-1974) in Iraq, and another Diploma in Cryptography from Switzerland in 1988. His main research interests include Wireless digital communication, cryptography, cryptanalysis, security evaluation, information hiding, digital watermarking, ICA, and soft computing techniques. He was the leader of many scientific research groups in different research institutes in Iraq from 1986 – 2003. He is the creator and the chair of IEEE Iraq Section since Sept. 2008- 2014 . He is the creator and chair of IEEE ComSoc Iraq Chapter since 2011. He is the Editor-in-Chief of 8 international scientific journals, and he is the Associate Editor-in-Chief of 6 international journals, and a member of 20 international scientific journals.