A Novel Approach of Message Encryption based on Steganography and Watermarking

Sonia Bansal
M.tech Scholar
DCSA, Maharshi Dayanand University
Rohtak, India

Sandeep Dalal, Ph.D
Assistant Professor
DCSA, Maharshi Dayanand University
Rohtak, India

ABSTRACT

Even after rapid development of encryption and decryption algorithms, the communication channels still face acute threat of illegal intelligence gathering. The science of steganography has also simultaneously emerged as a means of covert communication. One major reason is spread of digital images as means for passing classified information include the easy distribution, easy coping and simple means of modification. This is so vital that the aspect of image content modification and protection has become a major security issue. Recently, fragile watermarking has been used as a technique to achieve image authentication and tampering localization. The main purpose of this work is to present an algorithm for generation of stego file based on alternative watermarking. In this paper, we present an implementation of a fragile image modification scheme for classified communication. This scheme is based on chaos theory wherein a labile signal that is sensitive to modifications is embedded in the image so as to detect the image (and thus textual) tampering inconsistency. This approach can be implemented for content authentication.

Keywords

Cipher text, Cover image, Decryption, Encryption, Encryption Algorithm, Fragile watermarking, LSB, Plain text, Stego image.

1. INTRODUCTION

The standard and concept of “What You See Is What You Get (WYSIWYG)” that is generally encountered while printing images or other materials, is no longer precise and it does not always hold true. In today’s world the images are much more than what we see with our Human Visual System (HVS) and they are worth more than proverbial 1000 words. Steganography is the science of hiding confidential information within something innocuous. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information [3].

The steganography is often used together with cryptography. A steganography message (the plaintext) is first encrypted by some modern encryption algorithms, and then this encrypted data is embedded into some media file and sent to the receiver. The receiver then performs the operation of extracting the embedded data and then decrypts the data by making use of decryption algorithm. Modern steganography can be broken up into three categories: Pure Steganography, Secret Key Steganography and Public Key Steganography. Pure steganography is hiding information where no information other than the hiding technique is required, as this is sufficient knowledge to be able to retrieve the hidden message. The latter two categories, secret key and public key steganography, rely on the passing of a key (or keys) without which the hidden information cannot successfully be extracted. Most steganographic software available implements the secret key approach due to the facts that pure steganography is simple to break once you know the method and public key steganography is considered to be theoretically impossible.

Watermarking seems to be a complementary solution for image integrity and authenticity to other security mechanisms as cryptography [7]. Digital watermarking is a method that inserts some information into a multimedia object to ensure a security service and generates a water-marked multimedia object, which can be an image, audio, video or text [8]. Generally speaking, any watermarking scheme consist of several distinct parts: the watermark, the encoder which inserts the watermark on the multimedia object and the decoder which extracts the watermark in order to be useful for resolving a security service.

Watermarking techniques can be divided into different categories in various ways [7]. For instance, according to its work domain, watermarks can be embedded in either the spatial or the frequency domain; watermarks in this domain are more robust than those in the spatial domain. Also, watermarking techniques can be divided into four categories according to the type of multimedia object to be watermarked as follows: image watermarking, video watermarking, audio watermarking, and text water-marking. Based on human perception, digital watermarks can be divided into visible and invisible types. A visible watermark is a secondary translucent image overlaid into a primary image. On the other hand, the invisible water-mark is completely imperceptible by human perception, this kind of watermarks are commonly used because they preserve the visual quality of the watermarked object.

Finally, watermarking schemes can be classified in two types according its function: fragile steganography based on robust watermarking schemes, the latter is perhaps the most studied classification. Robust watermarking schemes are widely used for copy-right protection, i.e. ownership evidence. On the other hand, fragile watermarking schemes are used to address the authentication and integrity issues. Generally speaking, all fragile watermarking schemes can be classified into semi-fragile watermarking and complete fragile schemes according to integrity criteria [9], [10]. Semi-fragile watermarking based authentication is also called soft authentication. It allows certain content modifying such as JPEG compression. Complete fragile watermarking schemes are needed when any modifications of digital contents have to be detected. Such is the case of e-commerce, e-governance, law evidence, military and medical applications, all of these have high security requirements.

Taking this into account we may wonder, for example, whether it is preferable to use a fragile watermark, a robust watermark or even if is better to use a completely different technique, this partly depends on the type of multimedia object and its use.

This paper presents a novel algorithm in encrypting textual information inside an image which can be used for Content Authentication System - built upon the proposed fragile watermark. This new proposed fragile watermarking system is an extension of an existing secure data hiding scheme technique that is built on binary images [11]. It is considered as an excellent data hiding technique for binary image in terms of similarity and data payload. Kawaguchi and Eason proposed a data hiding technique in [6] - that embeds data inside bit planes of the gray scale image in accordance with the concept of pixel complexity which can be defined in different ways. The watermarking system that is proposed in this paper uses the first bit plane to embed an authentication signature using the binary image data hiding technique introduced in [11].

2. PROPOSED METHODOLOGY

In the selected scheme, the watermark is generated by pseudo-random chaotic process that involves the values of the original image pixels, i.e., its image content dependent. In order to extract an existing watermark in a watermarked image, the exact knowledge of system parameters is required. Additionally, if the image is not modified, the watermark can be completely removed from the original image.

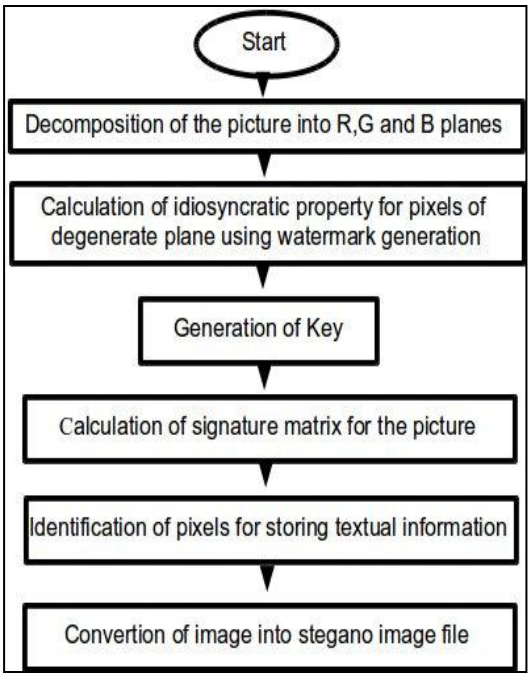
Start
Decomposition of the picture into R,G and B planes
Calculation of idiosyncratic property for pixels of degenerate plane using watermark generation
Generation of Key
Calculation of signature matrix for the picture
Identification of pixels for storing textual information
Convertion of image into stegano image file

Fig 1: Overall schematic of the programme for the generation of stego file.

Step 1: Generation of stego file

Here we describe each section of the information storing scheme: Picture decomposition into degenerate planes; Calculation of idiosyncratic property for pixels of degenerate plane, Generation of key, Calculation of signature matrix for the picture, Identification of pixels fit to store textual information, Conversion of image into stego image file.

Step2: Decomposition of image into degenerate plane: Images that use 24-bit colour scheme use 24 bits per pixel. In such images, each pixel is represented by three bytes, each byte representing the intensity of the three primary colours red, green, and blue (R, G and B), respectively. The algorithm presented in further sections here shall use least significant bits of the blue channels.

$$B = m\,[V_i]$$

Step3: Calculation of idiosyncratic property for pixels of degenerate plane using watermark generation:

The watermark generation process shall be applied on the spatial image domain, while scanning an image row wise, starting from the top-right corner of the image. For every pixel value an idiosyncratic property (S_i) shall be calculated and another matrix populated on its basis as follows:

$$S_i = f(S_{i-1}) + \alpha V_i \quad \ldots\ldots\ldots\ldots\ldots. \qquad (1)$$

Where $f(S_{i-1}) = \beta \mathrm{Sin}(\gamma * S_{i-1}) - \delta \mathrm{Cos}(\varepsilon * S_{i-1})$; Since the property S_i is dependent on S_{i-1} so for the starting pixel an arbitrary value (S_0) shall be chosen.

Step 4: Generation of Key:

The values of S_0, α, β, γ, δ, ε and the $f(S_{i-1})$ constitute the key which shall determine the incorporation of textual information, its transfer and eventual decoding.

Step 5: Calculation of signature matrix for the picture:

Using the values obtained in the property matrix of S, another matrix M shall be calculated such that

M_i = signature[S_i].. …………………… .(2)

Where, signature(S_i) = [1 if $S_i > 0$ or -1 if $Si \leq 0$].

Step 6: Identification of pixels for storing textual information:

In this step the pixels in blue plane shall be identified from matrix M_i such that the textual information is coded properly into the LSB. Only those pixels whose M_i value is 1 shall be considered. There shall be grouped into linear clusters of 8 pixels (starting from top right and moving towards left and down).

Step 7: Conversion of image into stego image file:

In LSB substitution method the textual data bits are hidden in the least square bits of pixels through LSB replacement. Let us imagine that the eight pixels have the following values

11010010

11001001

10010001

10000100

11001100

11000001

11001001

11001001

For storing information in the LSB of these pixels the substitution method shall be employed. Let us assume that an alphabet AM is to be sent. Since the binary depiction for A is 01100001 the LSBs of the first eight pixels (above mentioned pixels) shall be changed into

Non-LSB	LSB
1101001	0
1100100	1
1001000	1
1000010	0
1100110	0
1100000	0
1100100	0
1100100	1

For next alphabet i.e. M next set of eight pixels having M_i value of 1 shall be selected and then their LSB's replaced into "01001101" depicting M.

$S_{Ii} = S_i + I_i$...................... (3)

Where, S_{Ii} is Modified S property after information (I_i) has been added to the image.

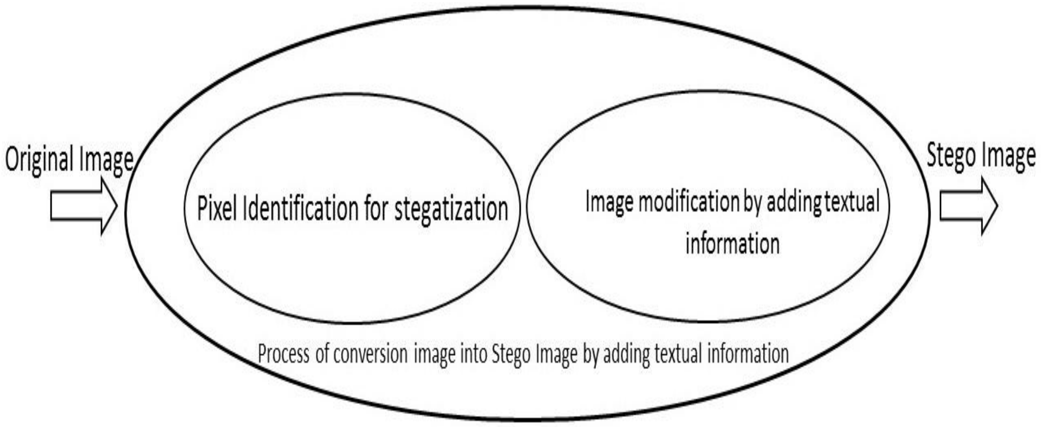
Original Image
Pixel Identification for stegatization
Image modification by adding textual information
Stego Image
Process of conversion image into Stego Image by adding textual information

Fig 2: Depiction of the embedding process of the image

3. CONCLUSIONS AND FUTURE WORKS

In this paper a novel algorithm is proposed for encrypting textual information in a picture format. The approach is based on the synergistic combination of watermarking and steganography. The usage of a periodic function (as in equation 3) in conjunction to the various modulating parameters like α, β, γ, δ, ε in the equation introduces pseudo-random character to the property S. Moreover the choice of signature matrix is another method to make the system even more stochastic. The selection of pixels by grouping of distant pixels leads to development of chaos in the selection process for pixels. The algorithm is simple yet very powerful and without the key it would take very large amount of energy to crack the encryption as extraction of the right information is only possible with correct keys. A person with wrong keys will not be able to obtain the S_i matrix. The current application can be improved if one also included other watermarking schemes, such as Fourier transform based robust schemes. Such implementation shall offer a very comprehensive copyright protection.

4. ACKNOWLEDGMENT

I would like to express my gratitude to my guide Dr. Sandeep Dalal for his valuable help and guidance. Finally I bow to the almighty, who gave me strength to carry out this work with sincerity and dedication.

5. REFERENCES

[1]William Stallings, "Cryptography and Network Security, Principles and Practice" Edition 3rd. Prentice Hall 2003, ISBN 0-13-091429-0.

[2]Kevin Curran and Karen Bailey "An evaluation of Image based Steganography methods" International Journal of Digital Evidence Fall 2003, Vol-2, Issue-2.

[3]A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, "Digital image Steganography: Survey and analysis of current methods" Science Direct Signal Processing 90 (2010) 727–752.

[4]R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography," J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474–481.

[5]F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," Proc. IEEE, vol. 87, no. 7, 1999, pp. 1062–1078.

[6]Kawaguchi E., and Eason R., "Principle and Applications of BPCS-Steganography," Proceedings of SPIE (3528), Multimedia satellite networks: issues and challenges, pp. 464-473, 1999.

[7]C. Rey, J. L. Dugelay, A survey of watermarking algorithms for image authentication, EURASIP Journal on Applied Signal Processing (JASP) 2002, pp. 613-621.

[8]E. Kougianos, S. P. Mohanty, R. N. Mahapatra, Hardware assisted watermarking for multimedia, Computers and Electrical Engineering, Vol. 35, No. 2, March 2009, pp. 339-358.

[9]S. Liu, H. Yao, W. Gao, Y. Liu, An image fragile watermark scheme based on chaotic image pattern and pixel-pairs, Applied Mathematics and Computation, 2007, pp. 869-882.

[10]Ming-Shi Wang, Wei-Che Chen, A majority-voting based water-marking scheme for colour image tamper detection and recovery, Computer Standards & Interfaces, Vol. 29, Issue 5, July 2007, pp. 561-570

[11] Tseng Y., Chen Y., and Pan H., "A Secure Data Hiding Scheme for Binary Images," IEEE Transactions On Communications, vol. 50, no. 8, pp. 1227-1231, 2002.