Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Hybrid Approach Crypto-Stegno Using Improved Chaos Based Sblock

Lata Bharti*, Dr. Sandhya Tarar, And Amita Dhariwal
School of Information and Communication Technology,
Gautam Buddha University, Gr. Noida, India

Abstract: ***In this paper a study on digital image/text crypto- stegano has been presented. In order to further strengthen the encryption of the distorted image, a steganography approach for data hiding is also proposed. Experimental results have exposed that the association and entropy values of the encrypted text before the addition are same to the values of correlation and entropy after the insertion. Since the correlation and entropy of chaos base spastically block have hiding essential data, the method offers a good disguise of the data in the encrypted text/image, thus decreases the chance of the encrypted text actuality detected.***
The first approach tries to overcome the targeted Steganalytic attacks. The work emphasis mainly on the first order data based targeted attacks. Two algorithms have been obtainable which can arrange the first order statistics of an image after embedding. The second approach aims at battling chaos based statically domain based Blind Attacks which try to estimate a model of the cover image from the stego image. Arithmetical Hypothesis Testing framework has been advanced for testing the efficiency of a blind attack and advances the effectiveness.

Keywords: Algorithm, cryptography, steganography, and Spatial desynchronization.

I. INTRODUCTION

The concept of steganography is to avoid illustration thought to the being of a hidden message. This method of information hiding has recently become significant in a number of ways. Digital audio, video, and pictures are increasingly equipped with unique but invisible marks, which may contain a hiding obvious notice or serial number or even help to prevent unauthorized replication straight.
Services infrastructures scheme make cumulative use of circulation security method, rather than simply hiding the satisfied message using encryption, seek to secrete its sender, its receiver or its very survival.
Comparable methods are used in some mobile phone schemes and proposed for digital selections. Some of the methods used in steganography are area tools or modest scheme such as minimum significant bit (R-LSB) insertion and noise operation, and convert area that include operation algorithms and image transformation such as discrete cosine transformation and wavelet transformation. However there are methods that segment the typical of both of the image and area tools such as patchwork, pattern block encoding, spread spectrum methods and masking.
Due to the fast growth of communication technology, it is suitable to obtain multimedia data. Unfortunately, the problem of illegal data access occurs every time and everywhere. Hence, it is significant to protect the content and the approved use of software data against the attackers. Data encryption is an approach to make the data unreadable, invisible or incomprehensible through broadcast by scrambling the satisfied of data.
In an image cryptosystem, it uses some consistent encryption algorithms or secret keys to convert or encrypt secret images into ciphered images. Only the authorized users can decrypt secret images from the ciphered images. The ciphered images are insincere and non-recognizable for any unauthorized users who grab them without knowing the decryption algorithms or the secret keys. "Steganography's place in security is to addition cryptography, not replace it. If a secreted message is encrypted, it must also be decrypted if discovered, which provides additional layer of protection."
Dissimilarly, stenographic methods denote to methods of embedding secret data into cover data in such a way that people cannot distinguish the being of the hidden data. The image stenographic methods (or called virtual image cryptosystems) are proposed to hide the secret images into readable but non-critical cover images. They are considered to reduce the notice of illegal users. Common methods for data hiding can be categorized into spatial and convert domain methods.

II. RELATED WORK

These overall study use the pixel gray levels and their color values directly for encoding the message bits and have to related study such as Spatial Domain and transform domain .

2.1 Spaticial Domain

Anderson Petitcolas and Craver, have both previously labeled ideas for public-key steganography. This employment will differ in numerous significant ways, do not challenge to give rigorous meanings for security, and give only experiential advices for the safety of their buildings. In contrast, we will stretch a hard meaning and proof of safety for public-key

steganography.

Petitcolas does not describe any device for making stego texts, but simply assumes "the ability to manipulate some bits of the cover". Craver assumes the being of a "supraliminal purpose" F and the ability to make a cover text which has F(x) = y for random y. In contrast, our model does not assume the existence of a function with non-standard properties, and is constructive. Confuses decoding with detection in its security argument. Thus they do not make clear what are the requirements on the underlying public-key cryptographic primitives.

2.2 Transform Domain

These techniques try to encode message bits in the F5 (Westfeld & Wolf, 1998) uses the Discrete Cosine Transform coefficients of an image for embedding data bits. F5 embeds data in the DCT coefficients by rounding the quantized coefficients to the nearest data bit. It also uses Matrix Encoding for reducing the embedded noise in the signal. F5 is one the most popular embedding schemes in DCT domain steganography, though it has been successfully broken in (Science & Goel, 2008).

2.3 Blind Attack Domain

The blind approach to steganalysis is similar to the pattern classification problem. The pattern classifier, in our case a Binary Classifier, is trained on a set of training data. The training data comprises of some high order statistics of the transform domain of a set of cover and stego images and on the basis of this trained dataset the classifier is presented with images for classification as a non-embedded or an embedded image. Many of the blind steganalytic techniques often try to estimate the cover image statistics from stego image by trying to minimize the effect of embedding in the stego image. This estimation is sometimes referred to as "Cover Image Prediction". Some of the most popular blind attacks are defined next.

(Goljan, Fridrich, & Holotyak, 2011). WAM uses a de-noising filter to remove Gaussian noise from images under the assumption that the stego image is an additive mixture of a non-stationary Gaussian signal (the cover image) and a stationary Gaussian signal with a known variance (the noise).

III. PROPOSED SYSTEM

The proposed renovation scheme is needy on the embedding scheme. The whole idea of embedding and restoring is that some of image pixels are used for embedding and rest are used for renovation. Fractional order systems are used for this resolve [30, 31]. The equations for global integer order.

$$x_1 = - x_1 - ax_2 - x_3x_2$$

$$x_2 = x_2 - bx_1 - x_1x_3$$

$$x_3 = cx_3 + x_1x_2 + 1$$

The Jacobian matrix at the equilibrium point

$E = (x_1,x_2,x_3)$ is given by

$$\mathbf{J} = \begin{pmatrix} -1 & -a - x_3 & -x_2 \\ -b-x_3 & -1 & -x_1 \\ x_2 & x_1 & c \end{pmatrix}$$

When, (a, b c) = (5, 85, 0.5), Volta's system shows chaotic behavior. For these restrictions, Volta's system has 3 equilibrium points.

3.1Algorithm Pixel Swap Embedding Research

The algorithm is summarized below.

Algorithm: Pixel Swap Embedding (PSE)

Input: *Cover Image (I)*

Input Parameters: *Message Stream (α), Threshold (€), Shared Pseudo Random Key (k)*

Output: *Stego Image Is*

Begin

1. (X1, x2) = randomize (i,k)
2. if $|x1 - x2| \leq €$
   thengoto step 3
   elsegoto step 1.
3. if $\alpha(i) = 0$
   if $x1 \geq x2$
   then swap(x1,x2) i = i+1
   else i = i+1
   goto step 1
   else goto step 4.
4. if $\alpha(i) = 1$

if x1 ≤ x2
then swap(x1,x2) i = i+1
else i = i+1
goto step 1
elsegoto step 1.
End *Pixel Swap Embedding*

The Randomize (I,k) purpose produces random non-overlapping pairs of pixels (x1,x2) using the secret key k public by both ends. Once a pair (x1, x2) has been used by the algorithm it cannot be reused again.
The statistical restoration algorithm is summarized below:

3.2 S-BLOCK (Low Detection Stegano-graphy) using Modified Steganography Algorithm

Algorithm S-BLOCK: Modified S-Steganography Algorithm (M S block)
Input:*Cover Image I*
Input Parameters: *Rows and Columns to be cropped (**u, v**), Block size (**m× n**), Quantization Matrix (Q)*
Output: Stego Image *Is*
Begin
1. Partition the cover image Ì into Î u, vand Ì u, v and $I^{\delta}_{U,V}$by cropping *u* topmost rows and *v* leftmost columns.
Let us denote this set of blocks by $P_{I\,u,\,v}^{(m \times n)}$
2. Select a set of blocks from $P_{\hat{I}\,u,\,v}^{(m \times n)}$ (using a key shared by both ends) and achieve the embedding in each of the selected blocks using any standard DCT based steganography scheme.
3. Perform $m \times n$ non-overlapping block partitioning on $\hat{I}_{U,V}$.
4. This quantization loss occurs for almost all the DCT domain embedding schemes. We try to avoid this problem by embedding data mostly in the low-frequency DCT coefficients.

3.3. Flow Diagram

This system can be clarified using the 'prisoners problem' (Figure 1.1) where Alice and Bob are two prisoners who wish to communicate in order to access an escape plan. However communication between them is inspected by the warden, Wendy. To send the secret message to Bob, Alice embeds the secret message 'm' into the cover object 'c', to obtain the stego object 's'. The stego object is then sent concluded the public channel. In a pure steganography framework, the method for embedding the message is unknown to Wendy and shared as a secret between Alice and Bob. In private key steganography Alice and Bob share a secret key which is used to embed the message. The secret key, for instance, can be a password used to seed a pseudo-random number generator to select pixel places in an image cover-object for embedding the secret message.

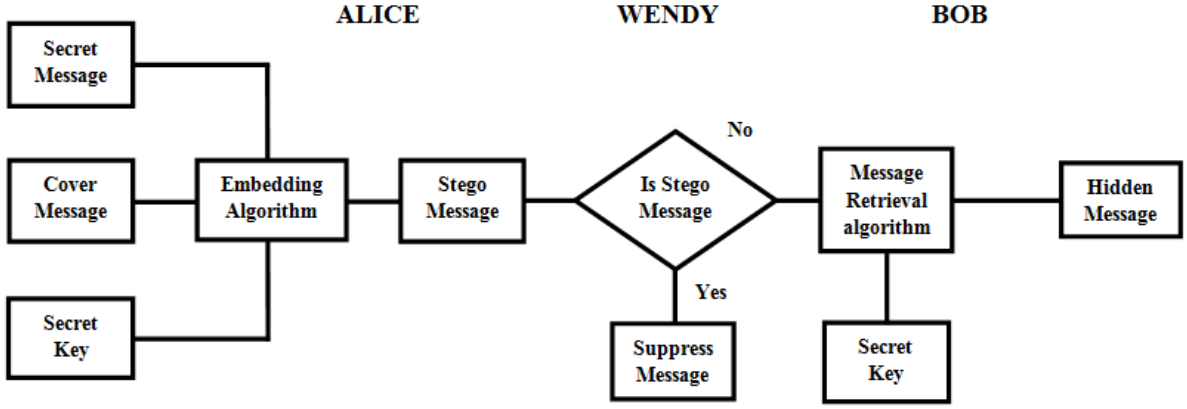

Figure 1 Flow diagram for proposed structure for crypto-stegno

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

The MSBLOCK algorithm has been exposed pictorial original cover image from which the cropped image Î u, v portion is labeled as EFGH is extracted. Î u, v is then divided into non overlapping blocks size $m \times n$ as shown by solid lines. A DCT domain stenographicstructure is then applied to some of these blocks and Î u, v is finally attached with $I^{\delta}u, v$ to get the stego image $\hat{I}_s$.

- Then the embedded image experiences JPEG compression before being connected to the decoding end, some of the embedded data bits might get lost in the procedure because of the quantization step through JPEG compression. Also embedded data can be made secure by adding some terminated bits in the data stream and using error-control coding methods. This problem of using error-control coding for securing the data bits has been addressed in (Solanki et al., 2009)albeit at the cost of *low embedding rate*. We would like to mention here that in our implementations of QIM, SSBA and SDSA we have not comprised any error-control technique. Let's associate the three schemes and verify our argument

Using Perfected outcome Hypothesis

Table 1: p-value of Rank Sum Test for 23 DCA

Embedding Rate(bpnc)	**QIM *p*-value**	**SSBA p-value**	**S-BLOCK:Low detection SDSA 8X8 p-value**
0.05	2.15×10^{-8}	0.0032	0.1380
0.10	0	2.24×10^{-4}	0.0065
0.25	0	1.12×10^{24}	4.23×10^{-6}
0.50	0	0	7.53×10^{-10}

Table 2: p-value of Rank Sum Test for Sblock

Embedding Rate(bpnc)	**QIM *p*-value**	**SSBA p-value**	**Sblock:Low detection SDSA 8X8 p-value**
0.05	0.1907	0.6947	0.8352
0.10	0.0059	0.6334	0.7833
0.25	1.028×10^{-16}	0.3270	0.5213
0.50	0	9.27×10^{-6}	0.3225

It can be seen that for all embedding rates the p-value of the SDSA algorithm is greater than the p-value of both SSBA and QIM system indicating that the SDSA algorithm produces a stego image population which is statistically closer to the cover image population than the populations generated by SSBA and QIM. It should be noted that even though the p-values obtained are small but for the determination of assessment it is meaningfully higher for the proposed system than that of QIM and SSBA

V. CONCLUSION

This factor bounds the applicability of this approach to only embattled attacks. The second approach studied in this research aims at hampering the steganalysts ability to efficiently approximating the statistics for organization. A new statistical model for testing the competence of calibration based blind attacks was proposed. It was found that the standardization step is indeed able to estimate an image model. To counter this, a comprehensive framework has been proposed which interrupts this model approximation of the attack. It is based on embedding data such that the stego people remains statistically quicker to the cover population and the variance between these two cannot be observed in the statistics drawn from the two populations. The framework was extended to a new algorithm for BMP domain steganography. This algorithm was assessed in the proposed statistical testing framework and it was found that the algorithm is positive in breaking the correction based blind attacks.

REFRENCES

[1] Sourav Dinda, " A New Approach to Secure Communication with Steganography and Cryptography", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 8, October 2013

[2] Sarita Poonia, Mamtesh Nokhwal, Ajay Shankar, "A Secure Image Based Steganography and Cryptography with Watermarking", International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-8, June 2013

[3] Hardikkumar V. Desai, " Steganography, Cryptography, Watermarking: A Comparative Study", Volume 3, No. 12, December 2012 Journal of Global Research in Computer Science

[4] R.Nivedhitha1, Dr. T. Meyyappan ,"Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology- Volume3 Issue3- 2012

[5] Khalil Challita and Hikmat Farhat," Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208 The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085

[6] Bhattacharyya, S., Banerjee, I., & Sanyal, G. (2011). "A Survey of Steganography and Steganalysis Technique in Image , Text , Audio and Video as Cover Carrier" (I. Banerjee, Ed.)Journal of Global Research in Computer Science, 2(4).

[7] Budiman, A. (2010). "Steganography Application On Video With Least Significant Bit (LSB) method".

[8] Piyush Marwaha1, Paresh Marwaha2," Visual Cryptographic Steganography in Images", 2010 Second International conference on Computing, Communication and Networking Technologies

[9] Dhawal Seth, L.ramathan, Abhishek Pandey," Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010

[10] George Abboud, Jeffrey Marean, Roman V. Yampolskiy, "Steganography and Visual Cryptography in Computer Forensic", 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering

[11] R.J. Anderson, F.A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal ofSelected Area in Communications, pp. 474-481, May 1998.

[12] Patterson & wayne (1998). "Mathematical cryptography for Computer scientists and mathematician", Roman & little field"

[13] A. Joseph Raphael, Dr. V. Sundaram, "Cryptography and Steganography- a survey" Int. J. Comp. Tech. Appl.., vol 2 (3), 626-630.

[14] Domenico Bloisi and Luca Iocchi, "Image based Steganography and cryptography", Dipartimento di Informatica e Sistemistica Sapienza University of Rome, Italy.

[15] Fridrich, J.; and Goljan, M. (2003). Digital image steganography using stochastic modulation. In Security and Watermarking of Multimedia Contents V, Vol. 5020, 191-202.

[16] Habes, A. (2005). 4 least significant bits information hiding implementation and analysis. ICGST Int. Conf. on Graphics, Vision and Image Processing (GVIP-05), Cairo, Egypt.

[17] R.J. Anderson, F.A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal ofSelected Area in Communications, pp. 474-481, May 1998.

