AN EFFICIENT SECURITY APPROACH USING PGE AND PARITY CODING

Ch. Rupa[1], P. S Avadhani[2], E. SrinivasReddy[2]

[1] Associate Professor, Dept of CSE,VVIT, Nambur,
Andhra Pradesh, India
{rupamtech@gmail.com}

[2] Professor, Dept of CS&SE, Andhra University, Visakhapatnam,
Andhra Pradesh, India
{psavadhani@yahoo.com}

[2] Professor, Dept of CSE, Nagarjuna University, Guntur,
Andhra Pradesh, India
{edara_67@yahoo.com}

ABSTRACT

Information Attacks are showing the weaknesses of Information security due to the rapid growth of the globalisation. The main aim of these attacks is to retrieve the information by illegal that shows the faults in the security services. In this paper, we introduce a novel secure steganographic approach for defending against these information attacks. In this approach, instead of original message an encrypted message by Prime Number and Gray Code Encryption (PGE) Algorithm is hidden into an Image (Stego Image) using a new approach named Linear Block parity coding (LBP) which provides more security than conventional approaches. The major strength of this paper is steganalysis has discussed. The computational complexity is comparatively low with other methods since our feature vector space is limited interference is not objectionable.

KEYWORDS

PGE, Steganography, LBP, Stego Image, steganaysis.

1. INTRODUCTION

Information is created, stored, processed and communicated using computers and networks. Computers are interconnected, creating new pathways to information assets. The threats to information are becoming more widespread and more sophisticated. Hence security has required for protecting the information. Many schemes were developed in order to protect sensitive data from adversary using either cryptography or Steganograpahy or both. Cryptography is an approach for encrypting or encoding the message bits using a key. Steganography is a technique to hide the secret message in a covert data. Steganography is more secure than cryptography [1].Various types of steganographic approaches are existed such as Text Steganography, Image Steganography and Audio Steganography. Here, Text steganography means protects the sensitive data (communicated data) by hiding into the covert Text data. Cheating Text approach [2, 3] is one of the examples to the above stated Text Stegography. Image Steganographic approach is a technique to hide the information into an image. Least Significant Bit (LSB) [4, 5] is one of the methods to hide the information into the image. To protect the information uses audio files in the audio steganography [6]. i.e Hidden the secret data in the audio files.

At the time of transmission of hidden text messages or hidden encrypted messages through remote networking, if the eavesdropper knows the track of the hidden text, then they could

DOI : 10.5121/ijdps.2012.3610

easily retrieve the text or encrypted text from covering media. If an encrypted message is retrieved by an attacker then original message can be achieved by applying Brute Force technique. So, there remains some probability of snooping of information. Hence these types of techniques sustain another level of security which can route the crypto analyzer or steganalyzer in a different direction. In this paper, proposed new heuristic approaches for encrypting the message that use Prime numbers and Gray Code Algorithm (PGE) and for hiding the information using Linear Block parity Coding (LBP) method [12]. It helps to improve the security of the transmitted message. This approach will satisfies all security services [7], improves the quality of control of cover media and progress the unintelligence (confusion) rate of an attacker.

The rest of the paper is organized as follows. We present Encryption Algorithm using Prime numbers and Gray code Algorithm (PGE) in section 3. Section 4 describes Steganography using LBP. The results and discussions and steganalysis with the existing methods are in Section 5.

2. RELATED WORK

Many techniques are proposed in the cryptography and steganography for optimizing the information security. Many symmetric encryption algorithms are proposed based on sensitivity of initial conditions using mathematical functions such as DES [7], Sierpienski triangle [16] using fractal geometry. Any symmetric encryption algorithm performs various substitutions and transformations on the plain text. Secret key is given as input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the secret key. Cipher text is the scrambled message produced as output. It depends on the secret key and plain text. Decryption algorithm is the encryption algorithm run in reverse. It produces the plain text by taking cipher text by taking cipher text and plain text [15].

In the text steganography, some text is used to hide either original text or cipher text such as cheating text technique [3]. This technique is required two major ingredients that are index table and Meaning full sentence which consists of all the characters which are existed in the data what are to be wanted to hide [13]. In the image steganography, original text or cipher text is hidden in the image using some methods such as Least Significant Bit (LSB) [13]. In this method, to hide data in an image the least significant bits (LSB) of each pixel is modified sequentially in the scan lines across the image in raw image format with the binary data. The portion, where the secret message is hidden is degraded while the rest remain untouched. An attacker can easily recover the hidden message by repeating the process [4,5]

Fig 1. General method to store

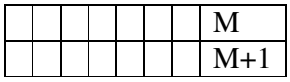

Fig 2. Least Significant Bit Approach

In this paper, we considered the best techniques existed with certain limitations and now overcoming them with suitable solutions using Prime number, Gray code and parity. In particular, we presented the importance of. We presented the importance of Graycode, Prime

numbers in the cryptographic approach and Linear block parity code for steganographic approach.

3. PROPOSED METHOD

In this approach, we used two security mechanisioms such as cryptography and steganography. To secure the message in the communication, encrypt the original message by using Prime numbers and Gray code Algorithm (PGE) i.e cipher text. This is a first layer of security. In the second layer of data security, cipher text is embedded into an image using LBP approach. This method satisfies all security services such as improves authentication through new encryption algorithm PGE and improves the confidentiality by LBP steganographic approach [12] and less chances to retrieve or modifying the messages in middle of the process i.e non repudiation, integrity and availability. Implementation of encryption algorithm (PGE) is as follows.

3.1. PGE Algorithm

This section consists of a message encryption algorithm which is done by Prime Numbers and Graycode [9].

3. 1. 1 Key Generation:

Perfun:

It is a random permutation function {1,2,...P}→ {1,2,...P}
Step 1: Let s_i is a starting bit of a key.
Where $1 \leq j \leq P$

Step 2: key = Sj + (size of a byte-1)

3.1.2. Encryption Algorithm

To encrypt original message into ciphertext using PGE algorithm is as follows.

Input: Plain Text
Output: Cipher Text
Step 1: Select text message as plaintext
Step 2: Generate Prime numbers (P[i]) from PIT to the plaintext.
Step 3: Find 9's complement to the Prime Number i.e Nine[i].
Nine[i] = Complement (P[i])
Step 4: Generate gray code (G_k) to complemented value (Nine[j]). i.e G_k
G_k=Gray (Nine[j]);
Step 5: Enc_i=G_k XOR Key

3.1.3. Decryption Algorithm

To enhance the original message from the ciphertext by PGE algorithm is as follows.
Input: Cipher Text
Output: Plain Text
Step 1: G_k = Enc_i XOR Key
Step 2: Convert G_k into Decimal.
D[i] = Dec(Bin(G_k))
Step 3: Apply 9's complement to D[i].
Nine[i] = Complement (D[i])
Step 4: Retrieve original message from PIT.

4. STEGANOGRAPHY USING LBP APPROACH

In the second layer of data security, cipher text is embedded into an image using Linear Block Parity coding (LBP) approach. In this approach, the binary image is the combination of Black and white pixel where black pixel is represented as '0' and white pixel is as '1'. It means, only one bit representation is possible for each pixel. As a part of building block parity data hiding method, first, considered an original image (I) represented by a matrix. It is partitioned into m x n blocks. To control the image quality after data hiding should be considered the following algorithm.

4.1. Data Hiding Algorithm

The original image 'I' is partitioned into m × n blocks. For simplicity, we assume that size of 'I' is multiple of m × n. The data hiding is achieved by modifying some bits of 'I'. Below we show how to hide one bit of original information into m × n host block, say 'a_i'.

Step 1: Find the parity of 'I'.
Step 1.1: If ((Sum (I_i) mod 2)==0)
then "Even Parity".
Step 1.2: If((Sum (I_i) mod 2)≠0)
then " Odd Parity".
Step 3: If ((Parity (I)=="Even") and
(a_i == 1)) ||
((Parity (I)=="Odd") and (a_i ==0))
then go to step 4 otherwise
"No change".
Step 4: Find Neighbor (I).
Step 5: Find the position of maximum value from Neighbor (I) to hide the data.
Step 6: Complement the bit in the position which we found in the step 5.

Embed the cipher text using the embedding algorithm LBP. The resultant image is called as stego image which is participating in the transmission. The results and analysis are discussed in the following section.

4.2. Case Study

Let us consider the m x n host block is as follows.

1 0 1 0 1 1
0 1 0 1 0 1
1 1 1 1 0 0
0 0 0 1 1 0
1 0 1 0 1 0

The linear block parity code for the m x n host block is identified by using simple parity identifier approach [12]. The resultant parity code of the m x n host is

m x n	Parity
1 0 1 0 1 1	0
0 1 0 1 0 1	1
1 1 1 1 0 0	0
0 0 0 1 1 0	0
1 0 1 0 1 0	1

The parity bit identifies the position of the data where it stores at the image. In this approach no need to transfer the location of the data bits by externally. Like this we can improve the security of the data. The same procedure is applied at receiver side to get the original information.

5. EXPERIMENTAL RESULTS AND DISCUSSION

Figure 3 shows the original image which is used to embed the secret message. Figure 4 shows the image in which data is inserted by LBP Steganographic approach using PGE algorithm.

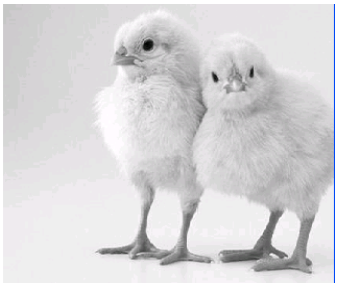

Figure 3. Original Image

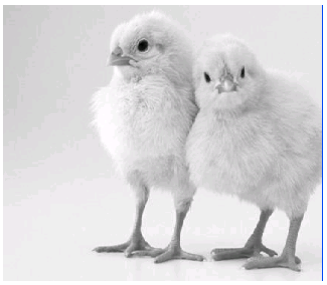

Figure 4. Stego Image

5.1. Steganalysis

Figure 5 shows the embedded message of sequentially embedded on top of the cover image since each bit from the message is sequentially ordered on the cover-image, then it will be easy for the third party to recover the message by retrieving the pixels sequentially starting from the pixel of the image [10, 14]. The embedded message of LBP embedding method is shown in Figure 6. In this approach, each bit is hidden by randomly instead of sequence order. The operations what we used in this approach like gray code, parity bit generation are found to require lesser time complexity as compared to any other logarithmic or exponential operations as in other encryption techniques and stego techniques.

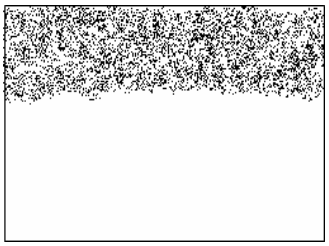

Figure 5. Sequential mapping of the pixel

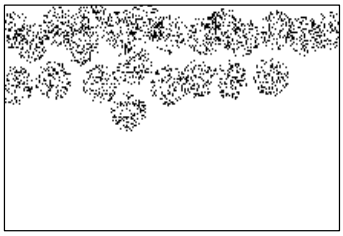

Figure 6. Linear block mapping of the pixel

7. CONCLUSION

Attacks on the information are a serious threat. A design of effective and efficient detection and response strategy is must. PGE with LBP solution successfully controls the attacks but has undesired impact on the legitimate flows. LBP is a new mechanisiom for hiding the information into an image. Compared to existing methods like least significant bit, it has taken less space to store the more information. After embedded information into a cover image, the resulting stego image will look identical to the cover image to the human eye. Further research is needed to refine the system.

REFERENCES

[1] Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE, (2004) Data Hiding in Binary Image for authentication and Annotation, IEEE Transactions On Multimedia, Vol. 6, No. 4.

[2] Ch.Rupa et. al, (2010) "Fast Comparison Encryption Scheme using cheating text Technique", International Journal of Engineering Science and Technology, Vol. 2(6), pp. 1725-1728.

[3] Chu-Hsing Lin and Tien-Chi Lee (1998) "A confused Document Encrypting Scheme and its implementation", Computer & Security, Vol 17, No.6, pp. 543-551.

[4] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, (2007) "Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4.

[5] Sutaone, M.S., Khandare, M.V (2008) "Image based steganography using LSB insertion technique", IEEE WMMN, pp. 146-151.

[6] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn (1999) "Information hiding – survey", Proc. IEEE, vol. 87, No. 7, pp. 1062 – 1078.

[7] Aamer Nadeem et al (2005) "A Performance Comparison of Data Encryption Algorithms", IEEE information and communication, pp .84-89.

[8] Johnson, N. F. and Jajodia, S (1998) "Exploring steganography: Seeing the unseen", IEEE Co puter Magazine, pp. 26-34.

[9] J. Sawad, (2007) "A simple Gray Code to list all Minimal Signed Binary Representation", J. Descrete Math, Vol 21, No. 1, pp. 16 – 25.

[10] Sos S. Agaian, Benjamin M. Rodriguez, Glenn B. Dietrich (2004) "Steganalysis using modified pixel comparison and complexity measure", pp. 46- 57.

[11] Bian Yang, Martin Schmucker, Wolfgang Funk, Christoph Busch, Sheng-He Sun: (2004) "Integer DCT-based reversible watermarking for images using companding technique", pp. 404-415.

[12] Xue-dong Dong, Cheong Boon Soh, Erry Gunawan, (1999), "Linear Block Codes for Four-Dimensional Signals", Vol .5, pp 57 -75

[13] Ch. Rupa et. al (2012) " Information security using Chains Matrix Multiplication", ICCSEA, pp. 703-712.

[14] N. Natarjan (2012) " Universal steganalysis using counterlet transform", Advances in intellegent and softcomputing, pp. 727- 736

[15] Buchmann, J.A. (2001) "Introduction to Cryptography", Springer, pp.71-74

[16] Alia, M.A., Samsudin, A.B. (2007) "Generalized Scheme for Fractal Based Digital Signature (GFDS)", IJCSNS International Journal of Computer Science and Network Security 7(7), pp: 67- 74.

[17] Rubesh Anand, P.M., Bajpai, G., Bhaskar, V.(2009), "Real-Time Symmetric Cryptography using Quaternion Julia Set. International Journal of Computer Science and Network Security" 9(3), pp. 20-26.

Authors

Dr. Ch. Rupa is working as Associate Professor in VVIT, Andhra Pradesh, INDIA. She has received B.Tech from JNTU, Hyderabad , M.Tech (CSIT) and Ph. D (CSE) degrees are from Andhra Uiversity. This author became a Life Member of CSI, ISTE, IAENG, IEI, IACSIT. She published more than 35 papers in various journals and conferences. JNTU kakinada had awarded her as a Young Engineer of 2010. IEI awarded her as National young Engineer of 2011 Govt of A. P and IEI by combined awarded her as Young Engineer of 2012. Her main research interest includes information security, Image Processing, Security algorithms.

Prof. P. S. Avadhani became a life member of CSI, ISTE, IAENG, IE, IEEE etc. He received his PhD degree from, IIT Kanpur, India in 1993. He is currently working as professor at Andhra University, visakhapatnam, INDIA. He had so many honors. He received best researcher award from Andhra University. He visited many other countires like USA Malysia, etc. Number of research scholars are enhancing their knowledge under his esteemed guidance. His main areas of interests are Computer Algorithms, Public Cryptographic Algorithms, Data Security, Computer Graphics, Fuzzy Systems.

Prof. E. Srinivasa Reddy received his PhD degree from, Nagarjuna University, India He is currently working as professor and Vice Principal at Nagarjuna University College of Engineering, Guntur, INDIA. He had so many honors. He presented his research papers in the prestigious conferences and published in the journals which are indexed by IEEE, LNCS etc. Numbers of research scholars are enhancing their knowledge under his esteemed guidance. His main areas of interests are Computer Algorithms, Public Cryptographic Algorithms, Data Security.