

A Novel StegoCrypt System using D-grid

D. Naga Tej¹ Ravi Kumar Balla²

^{1,2}Department of Information Technology

¹GVP College of Engineering (Autonomous), Visakhapatnam ²INFOSYS, Hyderabad

Abstract— Digitization has changed the face of the business applications. Digital media replaced all the traditional mechanisms. In particular business applications data exchange had to be done without the knowledge of the intruder. One such mechanism that accomplishes the goal is steganography. In this paper a novel method which double encrypts the message and then embeds it into a digital image using a D-grid is proposed. The proposed method preserves the quality of the image through a lossless approach.

Key words: Double Encryption, Data Grid (D-grid), Reference Grid (R-grid), Steganography

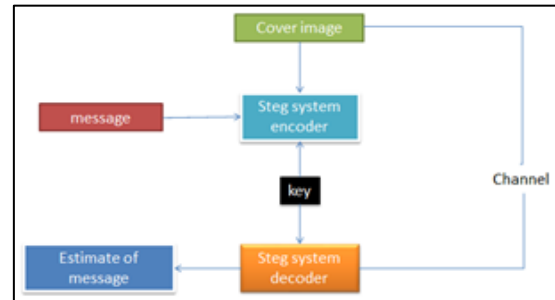


Fig. 1: Steganography

I. INTRODUCTION

In today’s age with the growth in information technology, traditional mechanisms are replaced by the digital media which increased the need for secure exchange of information. Cryptography provides the secure channel to exchange the information leaving the traces that some secret information had been shared between two parties, leaving the traces to the third party is to be avoided in confidential business applications. One such mechanism is steganography which hides the exchange of information from the third party.

Steganography’s goal is to keep its mere presence undetectable, but steganographic systems because of their invasive nature leave behind trivial traces in the cover image. Steganography alone is not sufficient to provide the required degree of security. Advantages can be obtained through hybrid system that combines the properties of both the systems like stego-crypt systems which encrypts plain text and then embeds the resultant into cover medium.

The main concern of this paper is to perform a secret secure exchange of the message (M). Secure exchange is acquired by double encrypting M with traditional cryptographic methods and secret exchange is gained through proposed novel steganographic approach

A. Steganography

Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper’s suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium’s redundant bits (those that can be modified without destroying that medium’s integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message.

B. Cryptography

In today’s age the primary objective is to keep the information secret from the unauthorized access of the intruder. One such technique to secure the information is cryptography. Cryptography involves converting the message into unreadable form known as cipher using encryption algorithms. The two basic algorithms are symmetric key cryptography algorithms and asymmetric key cryptography algorithms.

C. Symmetric Key Cryptography and Asymmetric Key Cryptography

For Symmetric key cryptography the sender and the receiver uses a shared key for encryption and decryption of the message. The sender encrypts the data using the shared key and then sends the cipher to the receiver who decrypts the cipher and extract the message using the shared key. The primary objective of symmetric key algorithms are used to hide a small key rather than large chunks of data. For Asymmetric key cryptography the sender and the receiver use different keys for encryption and decryption.

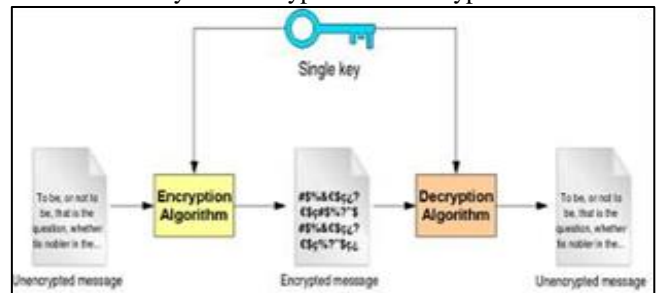


Fig. 2: Symmetric Key Encryption

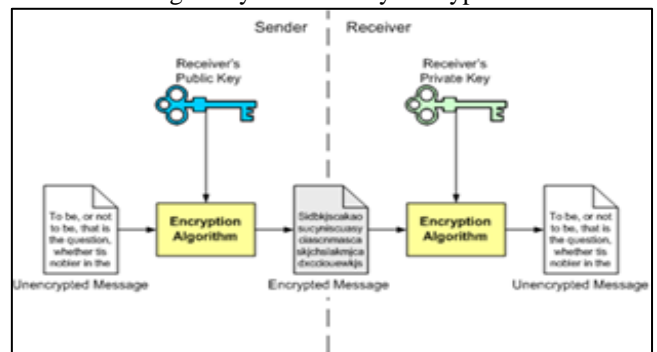


Fig. 1: Asymmetric Key Encryption

The two keys used are public key and private key. The sender encrypts the message using the receiver's public key. The receiver decrypts the message using his private key. Symmetric key algorithms are less complex and executes faster compared to asymmetric key algorithms.

D. Hybrid Cryptosystem

Hybrid cryptosystem is a more complex cryptography system that combines the features of symmetric and asymmetric key cryptography algorithms. We shall use asymmetric key cryptography techniques to convert the message into the cipher. For embedding the cipher into images symmetric key cryptography technique is used.

The remaining part of the paper is organized as follows. In section II proposed method is used. In section III architectures of proposed embedding and extraction scheme are presented. In section IV a brief description of the key and its analysis is described. In section V results are discussed and section VI concludes the paper.

II. PROPOSED METHOD

In this paper it is proposed to hide the presence of the message in the cover image based on the D-grid. A scheme for constructing D-grid from a symmetric key is proposed. To ensure the required degree of security, message (m) is double encrypted with conventional algorithms. Firstly, message is encrypted using an asymmetric algorithm followed by encryption with a symmetric algorithm. RSA and AES have been proving their significance in the field of cryptography from decades is selected as asymmetric and symmetric algorithms respectively.

$$C_R = E(\text{RSA}(M))$$

$$C_A = E(\text{AES}(C_R))$$

C_A is embedded into the image, based on the D-grid which is mapped from the Reference grid(R-grid). R-grid represents ASCII values in the form of a Two-Dimensional grid whose construction is based on a secret key.

	0	1	2	3	4	5	6	7
0								
1			\n					
2								
3								
4								
5								
6	0	1	2	3	4	5	6	7
7	8	9						
8		A	B	C	D	E	F	G
9	H	I	J	K	L	M	N	O
10	P	Q	R	S	T	U	V	W
11	X	Y	Z					
12		a	b	c	D	e	f	g
13	h	i	j	k	L	m	n	o
14	p	q	r	s	T	u	v	w
15	x	y	z					
.								
31								255

Table 1: R-grid with Key value $K_g=8$

A three dimensional D-grid is constructed where the dimensions one and two represent the corresponding location of the character in R-grid to identify concern pixel

and other dimension is embedding information (e) obtained from the position of that character in ' C_A '.

character	pixel co-ordinates	e
N	9 6	1
o	13 7	2
1	6 1	3

Table 2: D-grid mapped for text 'No1'

To maintain the correlation between the pixels of image the proposed embedded information in the range 0-9. A three step image preprocessing mechanism is proposed. In the first step the image is processed in such a way that no pixel contains the predefined pattern chosen in the key. In the second step image is divided into three layers. In the third step each layer is logically partitioned into block of size R-grid. The pixel chosen D-grid is modified so as to match the predefined pattern.

A layer is chosen based on the key values and corresponding RGB value is rounded and 'e' is embedded.

III. ARCHITECTURE OF PROPOSED SYSTEM

A. Embedding Scheme

The sender encrypts the secret message(M) twice to obtain cipher text(CT2). CT2 is mapped into a D-grid based on the R-Grid which is mapped on the preprocessed image to embed 'M'.

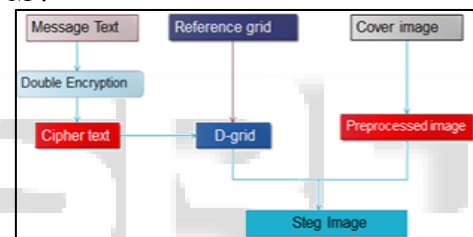


Fig. 4: Embedding Scheme

B. Extraction Scheme

The receiver traverses along the Steg image to identify the pixel set that contains 'CT2' based on the predefined pattern shared in the secret key, D grid is reconstructed from the pixel set. Receiver reconstructs the R grid from the key to remap the CT2 from the D grid. The 'CT2' is decrypted twice to obtain the secret Message 'M'.

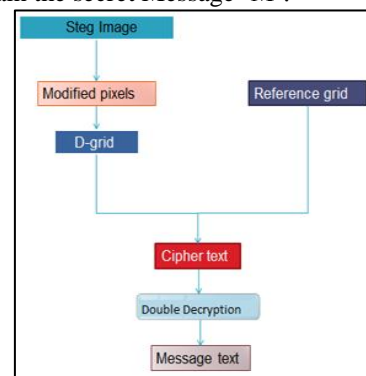


Fig. 5: Extraction Scheme

IV. KEY ANALYSIS

In the proposed method for ensuring the required degree of security 'M' is double encrypted with an asymmetric key followed by symmetric key algorithms. The length of the key depends upon those algorithms that are selected for

double encryption and an integer value of 8-bit is used for constructing the reference grid. To increase the security image is treated as 3 two dimensional layers with Red, Green, Blue. The order for embedding 'E' into the image is determined by a key value 'KO-order of layers' (3 bits) and a pre-shared order. Each bit determines whether to use or not to use the corresponding layer mentioned in the predefined order. State '0' of the bit mentions no change of the respective layer and state '1' mentions a variation in the predefined order. State '000' denotes circular right shift once and '111' denotes circular right shift twice, others represents no change in the predefined order.

K_0	Layer Order
000	BRG
001	RGB
010	RGB
011	RBG
100	RGB
101	BRG
110	GRB
111	GBR

Table 3: RGB Layers Order

V. RESULT ANALYSIS

A system is designed to implement the proposed method for various sizes of 'M' and images of respective size. The resultant steg image preserves the characteristics of the cover image and remarkable results are observed.

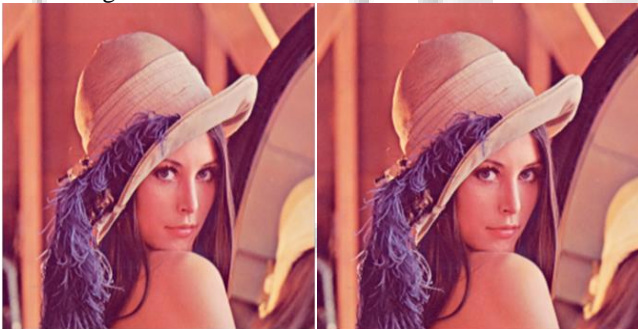


Fig. 7: Steg Image

VI. CONCLUSION

In this paper a scheme to secret secure exchange of a message is achieved in a lossless approach providing the required degree of security by double encrypting the message and embedding that into an image preserving the quality of the image. The proposed method acquires the strength of the conventional algorithms used.

REFERENCES

- [1] Piyush Marwaha, Paresh Marwaha, Visual Cryptographic Steganography in images, Second International conference on Computing, Communication and Networking Technologies, 2010.
- [2] Hide and Seek: An Introduction to Steganography, published by the IEEE computers Society, 1540-7993/03, IEEE 2003.
- [3] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997.
- [4] Bart Preneel, "Cryptographic Algorithms: Basic concepts and application to multimedia security", Katholieke University, Belgium