ISSN 2229-5518

Data Security Algorithm Using Two-Way Encryption And Hiding In Multimedia Files

Hamsa A. Abdullah

Abstract—In the current trends of the world, the technologies have developed so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another. There are many possible ways to transfer information using the internet: via emails, chats, etc. The data transmission is made very simple, speed and accurate using the internet. However, one of the main problems with transmitting data over the internet is the security threat it poses i.e. the personal or confidential information can be stolen or hacked in many ways. Therefore it is very important to take data security into consideration, as it is one of the most important factors that need attention during the process of data transmission. Data security basically means protection of data and providing high security to prevent data modification from unauthorized users or hackers. Data security has gained more attention in the recent period of time due to the massive increase in data transfer rate over the internet.

This paper proposing a new steganography method to hide any encrypted secret message in multiple steps. Firstly the secret message is encrypted by using Data Encryption Standard (DES) encryption method then the encrypted message is embedded inside one known image using Least Significant Bit (LSB) then the embedded host image is encrypted by using SCAN method. finally the encrypted cover image is embedded in final video file. Here the embedding and encryption done in two steps that make the system unbreakable foe sending password or confidential message.

Keyword— Data Security, Multimedia file, Encryption, Hiding, Steganography.

1 INTRODUCTION

With the development of the Internet, information processing technologies and the rapid development of communication, it is necessary to share information resources. Nevertheless, the Internet is an open environment so; information security has becoming increasingly important. The different embodiment disciplines of formation hiding are shown in following Fig. 1. Today, information security technology has two main branches, cryptography and information hiding. Cryptography process data into unintelligible form, reversibly without data loss. Cryptography aims to prevent unauthorized receivers from decoding the programs by scrambling them. Information hiding is divided into steganography and digital watermarking. Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. Steganography and cryptology are similar in the way that they both are used to protect important information The difference between the two is that Steganography involves hiding information so it appears that no formation is hidden at all. Nowadays the term "Information Hiding" relates to both watermarking and steganography.

Watermarking is the technique use to hide information in a digital object (video, audio or image) so that information is robust to adjustments or alterations. By watermarking, the mark itself is invisible or unnoticeable for the human vision system. In addition, it should be impossible to remove a watermark without degrading the quality of the data of the digital object. On the other hand, the main goal of steganography is to hide secret information in the other cover media (video, audio or image) so that other persons will not notice the presence of the information. Although steganography is separate and different from cryptography, but they are related in the way that they both are used to protect valuable information [1].

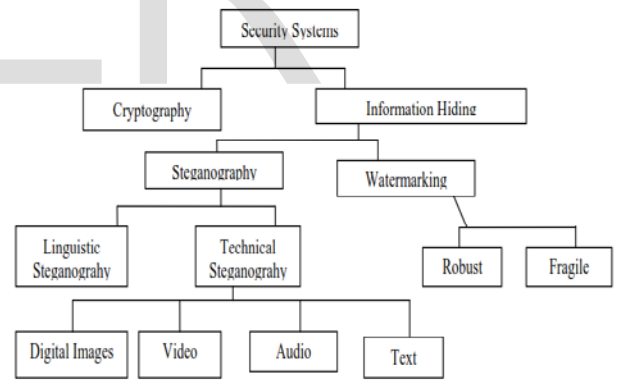

Fig. 1. The different embodiment disciplines of Information Hiding.

In this paper our proposed system uses both steganography and cryptography and provides double layer of security. the proposed system can be divided as the following steps:

Step 1. Encryption message by using DES.
Step 2. Embedding encrypted message by using LSB in cover image.
Step 3. Encryption cover image by using SCAN method.
Step 4. Embedding encrypted image by using LSB.

This paper is organized as follows. Section 2 describes the proposed system. Section 3 presents Simulation Results. The paper is concluded in Section 4.

ISSN 2229-5518

2 THE PROPOSED SYSTEM

Our algorithm works in four steps: Encryption message, Hiding message inside cover image, encryption cover image and embedding cover image inside cover video. Overview of these phases is given in the following Fig.2.

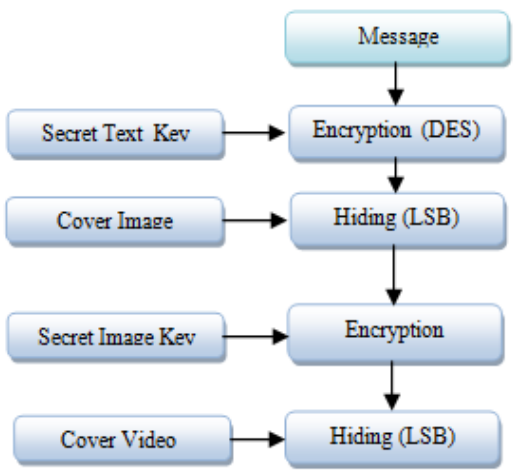

Fig. 2. The Proposed System

2.1 Encryption Message By using Data Encryption Standard (DES)

Step 1: An algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length.
Step 2: In this case, the block size is 64 bits.
Step 3: The block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme.
Step 4: The Feistel structure ensures that decryption and encryption are very similar process but the only difference is that the sub keys are applied in the reverse order while decrypting.
The Feistel (F) Function

The F-function, depicted in Fig. 3, operates on half a block (32 bits) at a time and consists of four stages:
Expansion

The 32-bit half-block is expanded to 48 bits using the expansion permutation, denoted E in the diagram, by duplicating half of the bits. The output consists of eight 6-bit(8*6=48bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the adjacent bit from each of the input pieces to either side.
Keymixing

The result is combined with a sub key using an XOR operation. 16 48-bit sub keys one for each round are derived from the main key using the key schedule.
Substitution
After mixing in the sub key, the block is divided into eight 6-bit pieces before processing by the S-boxes, or substitution boxes. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES - without them; the cipher would be linear, and trivially breakable [2].
Permutation

Finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the P-box. This is designed so that, after expansion, each S-box's output bits are spread across 6 different S boxes in the next round [3].

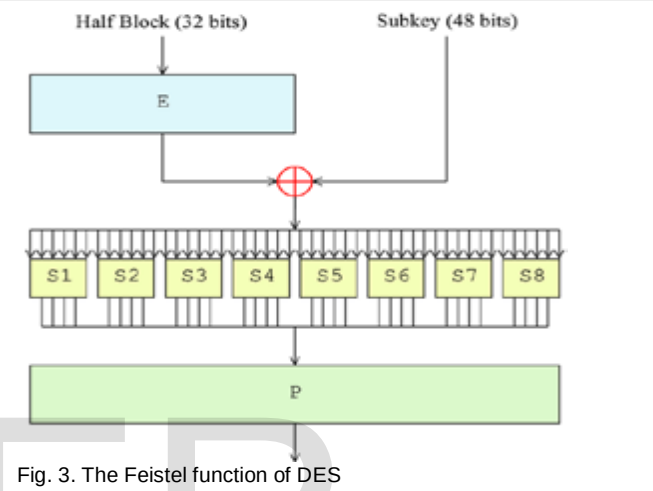

Fig. 3. The Feistel function of DES

Steps of Data Encryption Standard:
• Each block of message will be 64 bits. Do initial permutation on 64 bits data and divide it in to two halves.
• Left half 32 bits and Right half 32 bits.
• Expand right half up to 48 bits by expansion.
• Take 64 bits key (reduced to 56 bits by dropping bits at positions 8, 16, 24, …, 64) and select 48 bits by permuted choice.
• Do XOR of 48 bits right half and 48 bits key.
• Select 32 bits from step 5 by S-box substitution choice.
• Do P-box permutation (on 32-bits of step 6).
• Do XOR of 32 bits left half and 32 bits right half (from step-7)
• Result from step 8 will be new right half.
• Old right half from step 2 will be the new left half.

The above 10 steps make a cycle of DES. Step 1 to 10 is for one cycle. There will be 16 such cycles. After completion of 16 cycles, we have to do final permutation on data bits to get decrypted data. In simple
(L0, R0) ← IP (input)
Take a S-box function f : {0,1}48 x {0,1}32 -> {0,1}32 and 48-bit
string keys k1,k2,....k16 derived from the 56 bit key k, Repeat the following operation 16 times
Li = Ri-1
Ri = Li-1f (ki, Ri-1)
Output ← IP-1 (R16, L16)

ISSN 2229-5518

Embedding

1. For the embedding process the two files cover file and the secret file is chosen.
2. The secret file is encrypted to make it unreadable and more secure according to the choice of algorithm by the user.
3. Then the data of the encrypted data is converted to binary data where the file contains only the characters '0' and '1'.
4. Then for each space in the cover file the secret file is checked. the various cases for creating stego file are

If there is space in cover file and the secret file contains '0' then no change is done in the cover file.

If there is space in cover file and the secret file contains'1' then an extra space is added to the cover file.

5. Thus the indication of one space in the cover file represents the binary '0' whereas the indication of two space represents the binary '1'.
6. The resultant file is saved as the stego file [2].

2.2 Message Hiding in image using LSB

Least Significant bit (LBS) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the Red, Green, and Blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800*600 pixel image, can thus store a total amount of 1,440,000 bit or 180,000 bytes of embedded data [3]. For example, a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the LSB's of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover video [4].

In this work, the message may be a few thousand bits (8 bits per text character) embedded in million of other bits. Block diagram in Fig. 4 describe the general steps of concealing text in container image and reconstructing text hiding text file.

The following steps describe the details of 4-LSB steganography, in order to concealing secret text inside cover image, as shown in Fig..5.

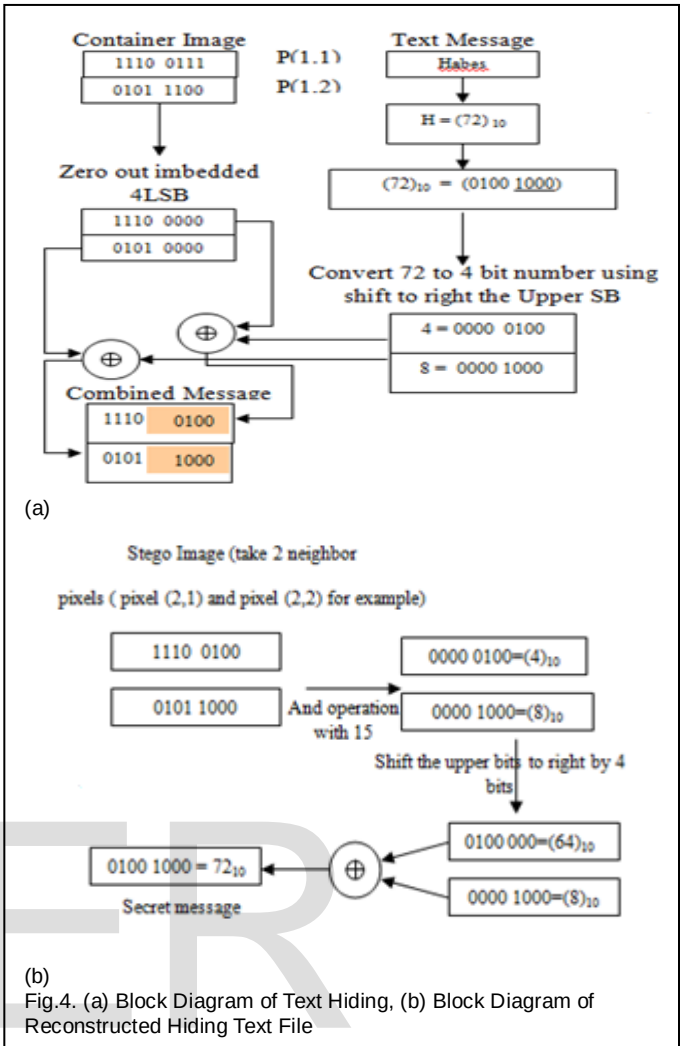

Fig.4. (a) Block Diagram of Text Hiding, (b) Block Diagram of Reconstructed Hiding Text File

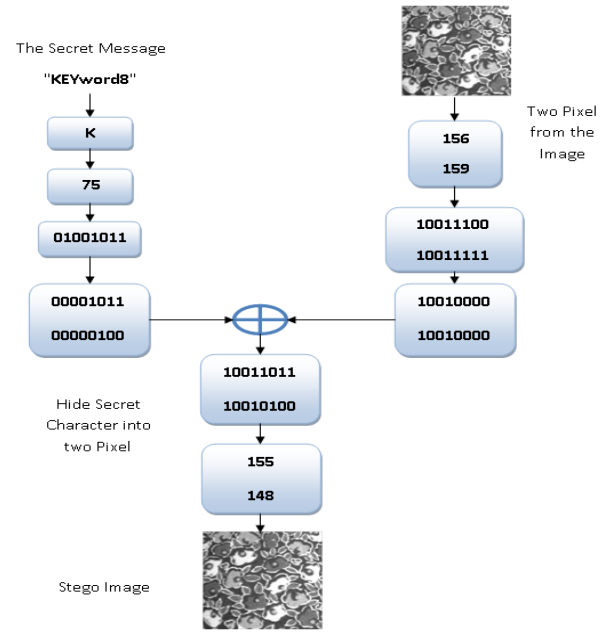

Fig. 5. Block Diagram of Text Hiding

ISSN 2229-5518

2.3 Image Encryption Using SCAN Encryption Method

A scanning of a two dimensional array is an order in which each element of the array is accessed exactly once. The SCAN is a formal language-based two dimensional spatial accessing methodology which can represent and generate a large number of wide varieties of scanning paths [5]. SCAN language uses four basic scan patterns. They are continuous raster C, continuous diagonal D, continuous orthogonal O, and spiral S as shown in Fig. 6. Each basic pattern has eight transformations numbered from 0 to 7. For each basic scan pattern, the transformations 1, 3, 5, 7 are reverses of transformations 0, 2, 4, 6, respectively.

To encrypt the image by using SCAN method we need create carrier image by using 4 out of 8 code. Here we are defining a new code called 4 out of 8 code. This code is of 8 bit length with 4 number of one's and 4 number of zero's and we made one consideration that each nibble must have 2 number of ones and 2 number of zeros. Since 26 alphabets (capital letters or small letters) and 10 numerals forms to give 36 alphanumeric characters, this code is more suitable to assign a unique code to each alphanumeric character [6]. Depending upon the keyword, carrier image is generated and used in the addition process to generate a encrypted image as shown in Fig. 7.

Encryption of an image can be done at different stage or multiple stages and in multiple ways. Fig. 8 show the block diagram of Image encryption by using Scan pattern with multiple keywords, where key-1 is corresponding to create a carrier image and key-2, key-3, key-4 along with SCAN encryption process are optional.

2.4 Image Hiding in Video using LSB

The following steps illustrate procedure of preparing video to hide text message in the LSB method .

- Read AVI video from its file location.
- Separate each frame of video sequence to its original color (RGB).
- Convert each of the colored plans to stream of binary bits.
- Use two adjacent pixels to hide one character from Red plan.

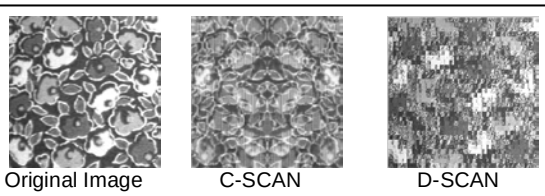

Fig. 6. SCAN Patterns

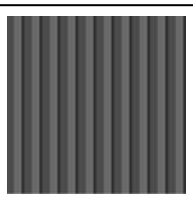

Fig. 7. Carrier Image with Keyword "INFORMATIONengineering2002"

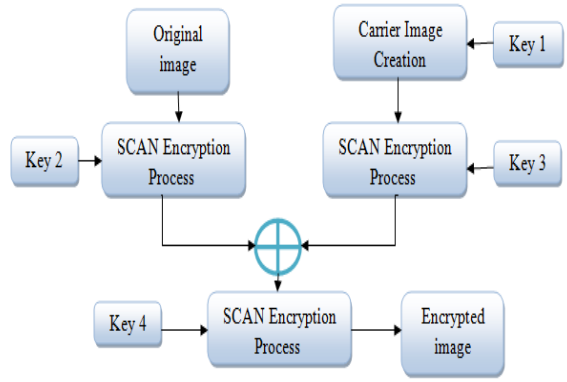

Fig. 8.Show the block diagram of Image encryption by using Scan pattern

- Read secret image that needed to hide in digital video.
- Covert each pixel in secret image to decimal number.
- By using AND operation can be divide secret pixel in to two half .
- Take the 4 upper significant bits alone; by perform shift operation by 4.
- Add the two half of the each pixel of the image to pixels of red plan (in 4 least bit) to the hide it in video frames by applying OR operation.
- Figure 9 show the proposed algorithm for image hiding in video by using 4-LSB.

3 SIMULATION RESULTS

In this paper the PSNR value is considered after embedding secret image inside video file. PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of a logarithmic decibel scale. A higher PSNR value indicates that the reconstruction is of higher quality..PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codes. The signal in this case is the original data, and the noise is the error due to hiding. The PSNR value is calculated by (1)

$$PSNR(dB) = 10 \times log\left(\frac{255^2}{MSE}\right)$$

Where MSE: Mean-Square error Mean Square Error (MSE): It is the measure used to quantify the difference between the initial and the distorted or noisy image and is given by (2).

$$MSE = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{\left(|A_{ij}-B_{ij}|\right)^2}{x\times y} \qquad (2)$$

Where x: width of image. y: height. x*y: number of pixels [7]. Table 1 show the results of the proposed system:

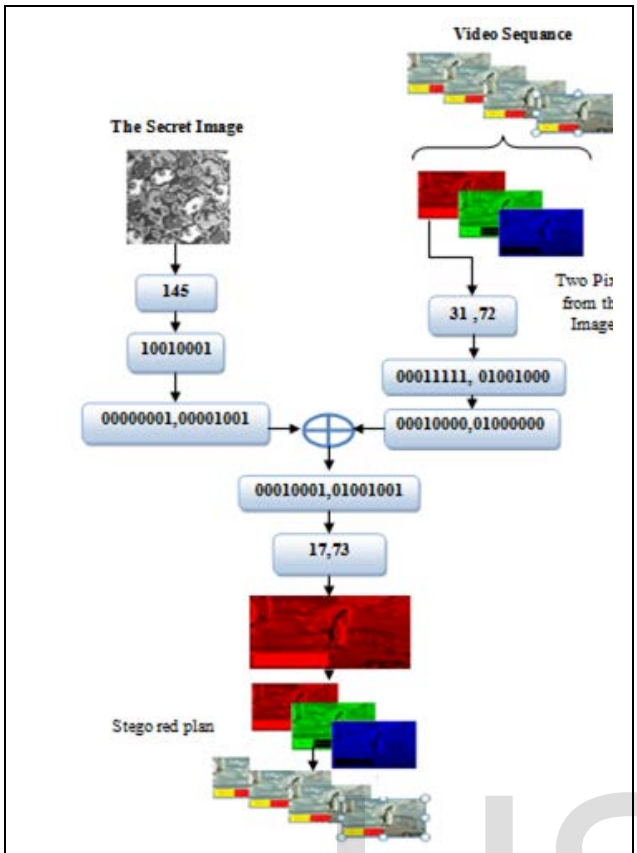

Fig. 9. The proposed algorithm for image hiding in video by using 4-LSB.

TABLE 1
RESULTS OF THE PROPOSED SYSTEM

The Secret Message	Encryption by DES with key " KEYword8 "	Hide with cover image	Encryption by SCAN	Hide with cover video	PSNR	Recover Message
INFOit12	\OF-=1$'				53.3234	INFOit12
inter10IT	\ot4&t%\				53.1730	inter10IT
None	None				Inf	None

4 CONCLUSION

The basic idea of the proposed algorithm in this paper to send secret password via secure multimedia file (image and video). The algorithm implemented by double two steps, the first two steps include encryption the password and hiding it inside image. The second two steps include encryption container image then hiding it inside cover video. This algorithm make the system unbreakable for sending password or confidential message and provide double layer of protection.

REFERENCE

[1] K. Venkata Ramana, Dr.B.Raveendra Babu, and Sri Ch.Ratna Babu, "A Randomized Secure Data Hiding Algorithm Using File Hybridization for Information Security", International Journal on Computer Science and Engineering (IJCSE), Vol. 3, No. 5, May 2011.

[2] V.Vijayalakshmi,P.Mahalakshmi, S.Thamizharasan, "Data Encryption hiding technique in non-standard cover files", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014) Vol. 2 Issue 1 Jan-March 2014.

[3] Hazem M. El bakry, Ali E. Taki_El_Deen , Ahmed Hussein El tengy, "Implementation of a Hybrid Encryption Scheme for SMS / Multimedia Messages on Android", International Journal of Computer Applications (0975 – 8887) Volume 85 – No 2, January 2014.

[4] T. Morkel, J.H.P. Eloff, M.S. Oliver, "An overview of image steganography", proceeding of fifth annual information security south africa conference, ISSA 2005.

[5] Rinkee Gupta , Jaipal Bisht, "Colour Image Encryption and Decryption by using Scan Approach", International Journal of software & Hardware Research in Engineering, Volume 1 Issue 2, October 2013.

[6] Panduranga H.T , Naveen Kumar S.K , "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images", (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 02, 2010.

[7] Harshitha K M, Dr. P. A. Vijaya, "Secure Data Hiding Algorithm Using Encrypted Secret message", International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012.