A Proposed Technique for Hiding Encrypted Data in Video Files

Mohamed El-bayoumy
Mansoura University, Egypt
Faculty of Computers and Information
Department of Information Systems

Mohamed El-mogy
Mansoura University, Egypt
Faculty of Computers and Information
Department of Information Systems

Ahmed Abou El-Fetouh
Mansoura University, Egypt
Faculty of Computers and Information
Department of Information Systems

Rasha El-Hadary
Mansoura University, Egypt
Faculty of Computers and Information
Department of Information Systems

ABSTRACT

Computer technology and the Internet have made a breakthrough in the existence of data communication. Securing the data transfer over a transmission media has become of great importance. This has opened a new way of implementing steganography to ensure secure data transfer. Steganography is the fine art of hiding the information. Hiding a message in a carrier file enables the deniability of the existence of any message at all. This paper proposes a steganographic technique to hide text data in a computer video file. The proposed data hiding system's objectives are: storage capacity, perceptual invisibility, strength against detection attacks and distortion resistance.

KEYWORDS

Steganography, Encryption, Least Significant Bit, Optimal Pixel adjustment Procedure.

1. INTRODUCTION

Encryption is the process of converting data (or information) in a way that eavesdroppers or hackers cannot read it, but the authorized parties can [1]. In an encryption scheme, the message or information (called plaintext) is encrypted using an encryption algorithm, turning it into an unreadable format (called ciphertext). This is usually done with the use of an encryption key, which determines how the message is to be encoded. An authorized party is able to decode the ciphertext using a decryption algorithm, which requires a secret decryption key that adversaries do not have access to. Cryptography's goal is to make communication unintelligible to those who do not have the right keys.

Steganography, or in other words, Data Hiding is a process that secretly embeds information inside a data source without changing its visual quality. Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message [2]. In data hiding, the actual information is not maintained in its original format and thereby it is turned into an equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated from it. The main idea of steganography is represented in figure 1. Steg analysis is the art of discovering and rendering such covert messages. Steganalysis needs to be done without any knowledge about the key used in embedding or even the algorithm [3]. Steganography, when combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication between two entities. This paper introduces a new technique combining encryption and steganography for more security requirements.

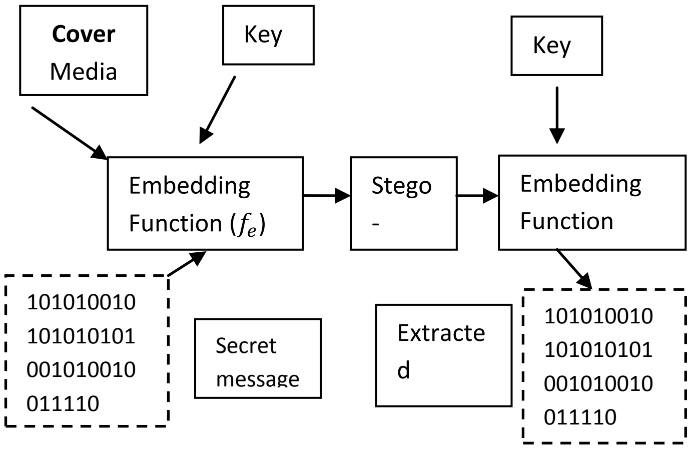


Figure 1: Data hiding block diagram

2. RELATED WORK

Encryption and steganography are considered nowadays two of the major scientific areas in the field of computer and digital security. Encryption is important because it allows us to securely protect data that we don't want anyone else to have access to. Businesses use it to protect corporate secrets. Governments use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft. Meanwhile, the purpose of steganography is covert communication to hide a message from a third party. The following subsections discuss some of the current encryption and steganography techniques.

2.1. Encryption Techniques

Many scientific researchers have been interested in the field of digital data encryption for purposes of security and safety of data transmission. For example, Sinha and K. Singh [5] have developed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using a suitable error control code, such as a Bose Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature can be used to authenticate the image. The advantage of the scheme is the authenticity verification. Increment in the size of the image due to added redundancy is the disadvantage of the algorithm. Also it does not have any compression scheme.

Panduranga H.T. and Naveen S.K [6] proposed a hybrid technique for image encryption which uses the concept of carrier image and SCAN patterns generated by SCAN methodology. Although it involves existing method like SCAN methodology, The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. The distinct advantage of simultaneous lossless compression and strong encryption makes the methodology very useful in applications such as medical imaging, multimedia applications, and military applications. The drawback of the methodology is that compression phase in addition to encryption takes longer time.

C. Chang et al. [7] used a popular image compression technique, vector quantization, to design an efficient cryptosystem for images. The scheme is based on vector quantization (VQ), cryptography, and other number theorems. In VQ technique, the images are first decomposed into vectors and then sequentially encoded vector by vector. Then traditional cryptosystems from commercial applications can be used. Major advantage of this algorithm is that it has a simple hardware structure. Required bit rate of VQ is small. Since VQ compresses the original image into a set of indices in the codebook, it provides saving a lot of storage space and channel bandwidth. The other advantage is that VQ has a simple hardware structure for providing a fast decoding procedure.

M. Bani-Younes and A. Jantan [8] introduced a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. Their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

2.2. Steganography Techniques

Least Significant Bit (LSB) modification [9] is perhaps the most popular method to embed a message into cover data. As its name suggests, LSB insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, 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 colour components can be used, since they are each represented by a byte. In other words, in each pixel 3 bits can be stored. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by normal human vision. This method is quite effective against human detection because it is difficult for the human eye to discern an LSB modified pixel. Also, any modifications that are made could easily be attributed to “noise” that may already be contained in the image. The advantages of LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many techniques use these methods. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB. The advantages of LSB techniques are: Popularity, Easy to understand and comprehend, High perceptual transparency, Low degradation in the image quality. However, there are few weaknesses of using LSB. It is very sensitive to any kind of filtering or manipulation of the stego-image .Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image will destroy the message. On the other hand, for the hiding capacity, the size of information to be hidden relatively depends to the size of the cover- image.

The Optimal Pixel adjustment Procedure (OPAP) [10] reduces the distortion caused by the LSB substitution method. In OPAP method the pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego image without disturbing the data hidden.

Fridrich [11] presented a new method for hiding message bits into the parity bit of close colors. The value of parity bit of the color R, G, B is determined as (R+G+B) mod 2. A message bit is embedded into each pixel of an image, by searching for the closest color entry in the palette until a color entry with the desired parity bit is identified. The parity bits of the palette entries that correspond to real images are more or less randomly distributed, guaranteeing that the original colors are not modified too much within the stego-image. However, the output stego-images generated by Fridrich’s method include false contouring and noise, especially when data is embedded in hand-drawn images (such as cartoon pictures):such images use only a few colors and so, the color difference between an entry and other entries is increased during embedding.

R.Amirtharajan et al. [12] proposed a steganography method for digital color image which employs a complete random scheme for pixel selection and embedding of data. Of the three colour channels (Red, Green, Blue) in a given colour image, the least two significant bits of any one of the channels of the color image is used to channelize the embedding capacity of the remaining two channels. This assures the uniform distribution of Mean Square Error, which gives better robustness and imperceptibility along with enhanced embedding capacity. The imperceptibility has been enhanced by suitably adapting optimal pixel adjustment process (OPAP) on the stego covers.

Pixel Value Differencing is used to provide a high quality stego image in spite of the high capacity of the concealed information. The number of insertion bits is dependent on whether the pixel is an edge area or smooth area. In edge area the difference between the adjacent pixels is more, whereas in smooth area it is less. While human perception is less sensitive to simple changes in edge areas of a pixel, it is more sensitive to changes in the smooth areas. This method [13] hides the data in the target pixel by finding the characteristics of four pixels surrounding it. After this tour in the previously developed methods in both encryption and steganography fields, let’s have a look at the proposed data hiding framework which will be presented in details in next section. The proposed system is a data-hiding method that uses high a digital video as a cover signal. The intended recipient needs only to process the required steps in order to reveal the message; otherwise the existence of the hidden information is virtually undetectable.

3. PROPOSED SYSTEM

The proposed scheme is a data-hiding method that uses high resolution digital video as a cover signal. The proposed recipient need only process the required steps in order to reveal the message; otherwise the existence of the hidden information is virtually undetectable. The proposed scheme provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms because here we consider application that require significantly larger payloads like picture-in-video.

The proposed model is composed of two phases: first phase, the encryption phase in which the secret message is converted into another format (usually a binary data) and here a previously known encryption algorithm will be used. The contribution will clearly appear in the second phase, Data hiding phase. The overall process of the proposed data hiding technique is divided into the steps shown in figure 2.

The data hiding system keeps pace with many necessary requirements: Embedding capacity, the amount of data that can be inserted into the cover-media without affecting its integrity. Perceptual transparency, to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media. Robustness, the ability of embedded data to remain intact if the stego-image undergoes various transformations such as scaling, rotation, cropping or compression. Tamper resistance, the difficulty to alter or forge a message once it is embedded in a cover-media, such as replacing a copyright mark with the one claiming legal ownership.

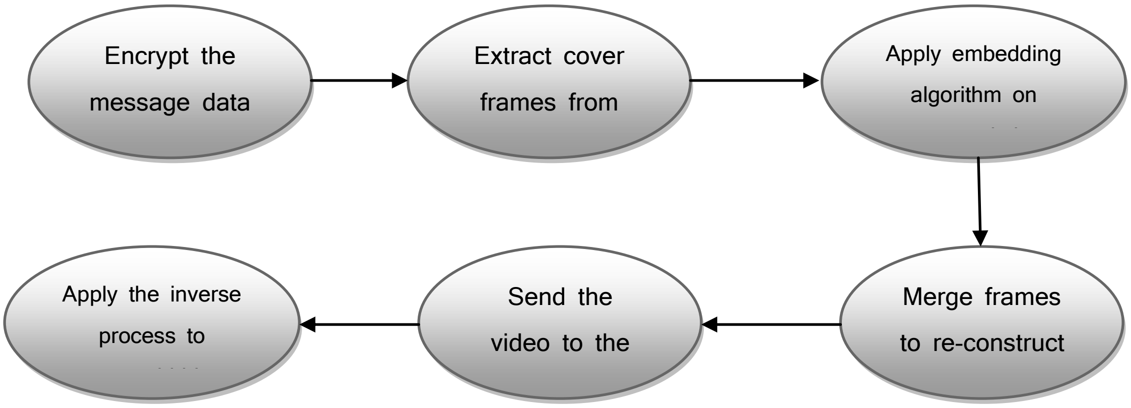

Encrypt the message data
Extract cover frames from
Apply embedding algorithm on
Merge frames to re-construct
Send the video to the
Apply the inverse process to

Figure 2: Data hiding steps.

The data hiding algorithm is detailed in the following steps:

Input: Cover image (I), Secret Text message (M)

Output: Text embedded image (I')

Step 1: Divide image I of size (M × N) into 3X3 pixel blocks,

If M%3 ≠ 0 or N%3 ≠0, Pad with additional zeros.

Step 2: Convert every letter of message M to its equivalent unicode series of bits so the message becomes Mb.

Step 3: Convert every pixel value of image I to its binary value (Pb).

Step 4: For each block B in image I:

Determine the minimum pixel value (Pbmin) in B

For pixel Pbmin: Set Pb = Pbmin

For pixels other than Pbmin: Set Pb = Pb - Pbmin (the difference D)

Determine the maximum D in block B (Dmax)

Step 5: Find the maximum difference of all image blocks Max (Dmax), then determine N = the number of bits enough to Save Max (Dmax)

Step 6: For each pixel in block B other than Pmin:

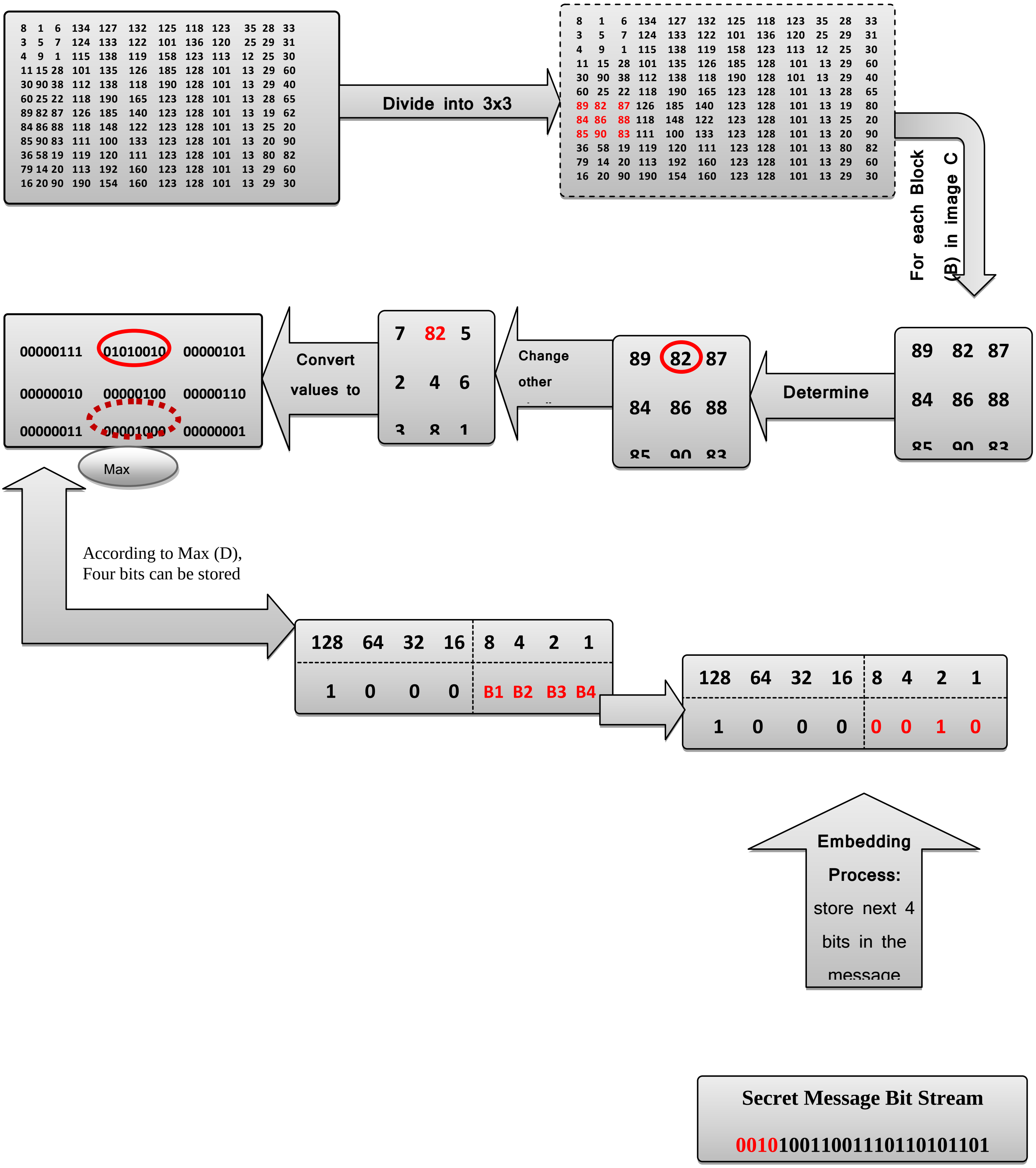
Swap the position of right-most N bits with the left most bits.

If Mb size ≠ 0: Set the new empty right-most bits to an equivalent number of bits in message Mb.

Step 7: Merge all the modified-pixels blocks into the new Image I'

A block diagram of these steps is shown in figure 3 below.

The data hiding system has many operational advantages: First of all is great storage capacity, by using bits in 8 out of 9 pixels of each block. Another advantage is invisibility, in other words any viewer may doubt in finding hidden data in an image, especially when it is distorted or not clear enough, but in case of a video, it may be considered a quality shortage of taking the video without concentrating on a special frame as frames are changed quickly. More security is ensured also as all people can view or download the video but only the intended person, who knows the embedding procedure and the extraction procedure as well, will analyze the video file – definitely some frames – to get the hidden message. No observed change in cover file size is an additional feature, adding data to an image file may make an observed increase in its storage size (especially when hiding large amount of data), but in case of video file there is no big difference in the clip's size. At last flexibility is realized as this technique can be performed in a similar way using an animation or any other time changing picture.



8	1	6	134	127	132	125	118	123	35	28	33
3	5	7	124	133	122	101	136	120	25	29	31
4	9	1	115	138	119	158	123	113	12	25	30
11	15	28	101	135	126	185	128	101	13	29	60
30	90	38	112	138	118	190	128	101	13	29	40
60	25	22	118	190	165	123	128	101	13	28	65
89	82	87	126	185	140	123	128	101	13	19	62
84	86	88	118	148	122	123	128	101	13	25	20
85	90	83	111	100	133	123	128	101	13	20	90
36	58	19	119	120	111	123	128	101	13	80	82
79	14	20	113	192	160	123	128	101	13	29	60
16	20	90	190	154	160	123	128	101	13	29	30

8	1	6	134	127	132	125	118	123	35	28	33
3	5	7	124	133	122	101	136	120	25	29	31
4	9	1	115	138	119	158	123	113	12	25	30
11	15	28	101	135	126	185	128	101	13	29	60
30	90	38	112	138	118	190	128	101	13	29	40
60	25	22	118	190	165	123	128	101	13	28	65
89	82	87	126	185	140	123	128	101	13	19	80
84	86	88	118	148	122	123	128	101	13	25	20
85	90	83	111	100	133	123	128	101	13	20	90
36	58	19	119	120	111	123	128	101	13	80	82
79	14	20	113	192	160	123	128	101	13	29	60
16	20	90	190	154	160	123	128	101	13	29	30

89	82	87
84	86	88
85	90	83

89	82	87
84	86	88
85	90	83

7	82	5
2	4	6
3	8	1

00000111	01010010	00000101
00000010	00000100	00000110
00000011	00001000	00000001

128	64	32	16	8	4	2	1
1	0	0	0	B1	B2	B3	B4

128	64	32	16	8	4	2	1
1	0	0	0	0	0	1	0

Secret Message Bit Stream

0010100110011101101101101

Figure 3: The proposed system's block diagram

4. EVALUATION

The next important stage is the evaluation of steganographic techniques. The steganographic methods will be evaluated by comparing the stego images with similar non-stego images. Similar here means that they are not the same but have the same content and lighting. Evaluators will look for patterns or unusual exaggerated noise. The patterns visible to the human eye could clarify the existence of a message. Another type of analysis involves comparing the original cover image with the stego-image in a number of ways. The palette will be examined. A reduced palette or noticeable pairs of colors in the palette will be looked for. A palette containing only 128 different colors should be easy to detect. The effects of embedding larger and smaller messages will be evaluated. Colour and grayscale images will be compared. Four distinct but complementary methods of evaluation are:

Pattern Analysis of Image Pixels: This detection method is based on looking for patterns in the bits that make up the pixel colors. For example if methods hide messages in the least significant bits of pixels then looking for patterns in the least significant bits of pixels is an easy way to detect the existence of messages. There are many variations of this message hiding technique such as hiding the message bit in the least significant bit of either the red, green or blue value of the colour or the parity bit of the pixel.

Pattern Analysis of Image Palette: This detection method is based on looking for patterns in the images palette. For example some steganography methods require an image with a reduced number of colors. The steganography methods then create new colors that are almost identical to the existing ones but have different least significant bits or parities.

Visual Inspection of the Image: This analysis method is based on evaluation through visual inspection of the image by independent evaluators. In all cases, the steganographic methods create a degree of distortion in the image, due to the reduction in the number of colors or the mixing and matching of existing colors.

Low Level Visual Inspection of Image Pixels: This detection method is based on carrying out a detailed inspection of selected sections of an image at a high degree of magnification to determine whether anomalous patterns become apparent. As an inspection technique this might be problematical if the original cover image is not available for comparison.

A comparison between the proposed technique and two other major techniques is presented in Table 1.

Table 1 - comparison between steganography techniques

	LSB	Statistical Techniques	Proposed technique
Imperceptibility	High	Medium	High
Robustness	Low	Low	Medium
Payload Capacity	High	Low	High

5. CONCLUSION

In this paper a data hiding technique for image and video files is proposed. The main intension is to provide proper protection on data during transmission. Its main advantage is that its effect on video quality or coding efficiency is almost negligible. It is highly configurable, thus it may result in high data capacities. Finally, it can be easily extended, resulting in better robustness, better data security and higher embedding capacity.

6. REFERENCES

[1] O. Goldreich, 2004. "Foundations of Cryptography: Volume 2, Basic Applications". Vol. 2.Cambridge university press.

[2] Debnath Bhattacharyya, P. Das, S. Mukherjee, D. Ganguly, S.K. Bandyopadhyay, Tai-hoon Kim,2009."A Secured Technique for Image Data Hiding", Communications in Computer and Information Science, Springer, Vol. 29, pp. 151-159.

[3] BablooSaha and Shuchi Sharma, 2012.Defence Science Journal, Vol. 62, No. 1, pp. 11-18.

[4] The steganography basics (http://www.infosyssec.com/infosyssec/Steganography/basics.htm), last accessed 12-02-2013.

[5] AlohaSinha, Kehar Singh, 2003. "A technique for image encryption using digital signature", Optics Communications, Vol-2, pp 229-234.

[6] Panduranga H.T, Naveen Kumar S.K,"Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images", International Journal on Computer Science and Engineering Vol. 02, pp. 297-300, 2010.

[7] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software, pp 83-91, 2001.

[8] Mohammad Ali BaniYounes and AmanJantan, 2008. "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35.

[9] FrankHartung, Martin Kutter, 1999. "Multimedia Watermarking Techniques", Proceedings of the IEEE, Vol. 87, No. 7, pp. 1085 – 1103.

[10]C.K. Chan, L.M. Chen, 2004." Hiding data in images by simple LSB substitution", Pattern Recognition, Vol.3, pp. 469-474.

[11]Fridrich, J.,''A new steganographic method for palette-based images1999 ''. IS&T PICS, Savannah, Georgia, pp.285–289.

[12] R. Amirtharajan, Sandeep K. Beher, Motamarri A. Swarup, Mohamed Ashfaaq, John Bosco and Balaguru Rayappan. 2010. "Colour Guided Colour Image Steganography", Universal Journal of Computer Science and Engineering Technology, Volume 1, pp.16 – 23.

[13] C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, 2008. "A high quality steganography method with pixel-value differencing and modulus function", J. Syst. Software 81, pp. 150–158.