Journal of Theoretical and Applied Information Technology
30th June 2019. Vol.97. No 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# A NEW ROBUST APPROACH FOR SECURING DATA TRANSMISSION

**NIDAL M. TURAB[1], JAMAL ZRAQOU[2]**
[1]Faculty of Information Technology, Al-Ahliyya Amman University,
Amman-Jordan
[2]Faculty of Science and Information Technology, Al-Isra University
Amman-Jordan
E-mail : [1]n.turab@ammanu.edu.jo , [2] jamal_sam@iu.edu.jo

**ABSTRACT**

Much research work is conducting to find algorithms for embedding hidden information that contribute in the fields of developing watermarking and steganography. The research work introduced in this paper aims to propose an approach for sending data securely by embedding a hidden cypher text in a stream of images. This study presents an algorithm for hiding information in key frames of a coloured video and then retrieving these data securely and efficiently. Two things should be taken into account, the embedded information should be invariant to the possible changes that might occur for video conversion from one format to another and not all the video frames will be used for hiding the information. Consequently, this research will focus on how to recover the exact version of the original frame in case of any manipulation or update.
The proposed work can be divided into two parts, the first one is applying a data encryption method to generate ciphertext, and the second part is to embed the cypher text into frames of a video. The proposed algorithms then are being able to retrieve the original text from the frames efficiently and securely. This research study focuses on contributing more knowledge in both fields.

**Keywords:** *Encryption, Decryption, Embedded Key, Transform Coding*

## 1. INTRODUCTION

Watermarking is the science of embedding information into signals such as images, videos etc., which is found to be a solution for protecting the copyright of assets and for data authentication. The embedded information can be visible or invisible to users. On the other side, steganography is an art of sending a secrete message under the camouflage of a carrier content [1].

Steganography is linked to the problem of hidden channels. Ideally it is preferable to send openly encrypted electronic files or mails to each. Consequently, there are some situations this case is not possible, maybe because the policy of the involved company does not permit encrypted email or the local government is declining the encrypted communication. Steganography is considered as one of the best solutions for this case.

Steganography is a continuous growing field of research. The work introduced in this paper aims to contribute in the area of steganography by introducing a new method to hide text in frames of a video and then being able to retrieve it securely and efficiently.

The main problem that this paper tends to tackle is the possibility to send text securely from the sender to the receiver with less risk of data discovery from unauthorised users. The transferred text should be invariant to changes during the transmission phase

This research is composed of four main sections: section 1 illustrates the introduction and the problem statement of this work, also provides the main aim of this research by developing the production of text hiding. Section 2 provides an overview of related works with regards to text hiding. Section 3 introduces the proposed methodology by introducing several methods to achieve the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

reliability of text hiding. Finally, the conclusion and future works are illustrated in section 4.

## 2. LITERATURE REVIEW

The main focus of this research on conveying secret message securely over a video by employing both watermarking and steganography techniques to achieve the aim of the study. A review for both fields is presented in this section. The first part presents the watermarking review followed by a review for the steganography.

The use of watermark dates back to 1282, where it is used at Bologna, Italy to mark paper of company [1]. Then it is common in practice up to 20th century. After that watermark also used in the postage stamp and currency notes of any country. The use of a mark then is widely used for postage and to protect the currency notes for each country. Not until the end of the 20th century, the Digital watermarking was presented as an approach for securing digital assets such as digital images, audio, video [2].

There are two main steps in watermarking for digital images which are embedding the watermark in the original image to create the watermarked image and then being able to extract the watermark from the watermarked image. Surveying the literature in digital watermark for digital image protection show that several studies were introduced, each study presents different methodology which adapts to particular type of images. Since the focus of this study is on digital watermark, a survey for art of work studies in this field is introduced in this section.

Many research studies in the area of digital watermarking and steganography were introduced mainly based on the algorithm of overlaying of two of halftone images. The procedure followed in this method depends on using binary watermark images, and a correlation is applied for each pixel on the two half tone images which matches to an on pixel on the watermark image. However, this algorithm reveals two main drawbacks which are the watermark is a binary and thus does not provide thorough features, and which add restrictions on the watermark images to be a kind of simple graphics such as logos. The second drawback is that the reliability of the image is low due to the presence of patterns from both image when the watermark is extracted. A study for tackling both of the aforementioned drawbacks is introduced in [3]. The proposed algorithm can be applied on images with multiple levels of grey scale instead of just applying on black and white images. Moreover, the algorithm can be applied on colour images. Extraction watermark is conducted using more general functions.

Stochastic screen patterns were used to create watermarks in reproducible documents in [4]. The algorithm includes four main steps; firstly, a stochastic screen pattern is generated for recreating a grey scale image on a document. Secondly, finding minimum one definitive stochastic screen description for the first stochastic screen pattern. Thirdly, generating a document includes the first stochastic screen. Fourthly, generating another document includes one or more of the stochastic screens. In this manner overlaying both documents in order to display them simultaneously results in correlating the first stochastic pattern on both documents due to using the first screen. On the other hand, no correlation takes place in areas where the area where the derived stochastic screens take place and as a result, the image exists therein using the derived stochastic screens becomes visible.

A method for digital watermark is presented in [5]. The method adapts to multiresolution images. In the proposed watermark embedding algorithm, the image is decomposed into its n-level wavelet decomposition coefficients, wavelet coefficients are used for embedding the watermark signal in the original image. A threshold value is used to prevent the human eye from recognizing the embedded watermark in the received image. The algorithm was evaluated by conducting several experiments, the results introduced that the methodology is adaptive to multiresolution images, and preserves the image quality.

Another algorithm for digital watermarking in frequency domain was introduced in [6]. The mechanism of the proposed method is based on using non-maximal pseudorandom sequences to define a ring of coefficients. The watermark is hidden in the coefficients distributed along the ring. For each watermark bit for a specific number of the existing coefficients, the longest available sequence was calculated. Moreover, the efficiency of the proposed algorithm versus the security performance of the encoding process. The extra parameter is used

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to determine the size of a subset of existing coefficients in the transform domain which was used for hiding the watermark in the image. The performance of the algorithm is evaluated by conducting several experiments which show that the algorithm is efficient towards several geometric transformations and image processing functions.

In [7] a method was designed based on using the low-frequency band of Discrete Cosine Transform (DCT) coefficient which is achieve by combining DCT and Principal Component Analysis (PCA). Experimental results show that the presented algorithm is robust to variety of image processing operations such as JPEG compression applied with several quality factors and low pass filter.

Several studies in the literature were built based on using Huffman coding [8], which is proved to give more robustness watermark results [9]. In [10] a random image matrix is used to create a watermark for the original image, and then the watermark is added to the original image. For watermark detection, the reverse procedure is used to find the water mark. The proposed algorithm was tested on greyscale image which have less than 245 greyscale pixel value.

A commutative encryption and watermarking approach was introduced in [2]. The encryption and watermarking are added during advanced video coding phase. The proposed algorithm applies encryption to the (DCT) coefficients' signs, motion vector difference and the intra-prediction mode during the H.264/AVC compression process. Moreover, an adaptive watermarking is applied to the DCT coefficients' amplitudes.

Generally speaking, steganography represents invisible communications, by hiding information in another media such as images, audio, video…etc. There are two main parts in Steganography, the cover medium used for hiding the information which can be any type of medium such as text, image, audio, video, etc.… and the secret message to be transferred over the cover medium, which also could be any type of medium as in the cover medium. A review for some research studies conducted in steganography is introduced in the following paragraphs of this chapter.

A text based steganography algorithm was introduced in [11]. The algorithm is mainly designed for Persian/Arabic text steganography, where a vertical displacement of the points is applied to hide the information inside the text.

An algorithm for image steganography based on block DCT and Huffman encoding was introduced in [12]. The algorithm is applied mainly on grey scale cover image which is divided into 8x8 blocks and then a two-dimensional Discrete Cosine Transform is applied on each block to transform to frequency domain. The next step of the algorithm includes applying Huffman encoding into the stenographic image which represents the secret message. The process of embedding each bit of Huffman code of the secret image in the frequency domain of the cover image is achieved by altering the least significant bit of each of the DCT coefficients of each block in the cover image. The algorithm was evaluated by conducting experiments which show that the algorithm can perform well and securely comparing to other existing methods. Another algorithm for image-based steganography was presented in [13]. The algorithm works on RGB colour images, where each channel of red, green and blue for each pixel is used to hide a different number of bits of the secure message. The number of stored bits increases by decreasing the number of colour component. Experimental results reveal that the algorithm satisfied results comparing to similar algorithms. To overcome the dimension limit for embedding resulting from using image as a cover medium for hiding the information, several studies were conducted to use video as a cover medium. Some of these studies is introduced in this review.

A Lazy Wavelet Transform Based Steganography in Video was presented in [14]. A modified encoding technique is applied to transform the video using a lazy wavelet transform, followed by using LSB encoding scheme on the sub bands of the video. The algorithm takes advantages of the visual and audio component of the video, where the information is hidden in the visual component and the audio component is used to hide the length of storing by applying LSB. Another video based steganography algorithm was introduced in [15]. In this study, the cover medium is a video and the secret message is a video as well. MATLAB is used for implementation. A Deoxyribonucleic Acid (DNA) properties-based steganography algorithm was introduced in [16]. The method in this study includes converting the video into frames, and then least significant bit substitution technique is used to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

hide the message in random places inside the randomly selected frames. Experimental results show that the algorithm causes some degradation in the video file.

In [17], two techniques were used to perform steganography over video file. The first method used for hiding data is the Random byte hiding, where lines of the frame is used for hiding the information at different location known only to authorized receiver. The second technique used is LSB which is used for embedding information in each pixel of the frame.

In [18], the algorithm starts by converting the video into frames followed by applying single level discrete wavelet transform on selected frames and on the image, which represents the secret message. Encoding and decoding the secret data is done using Arnold function where a private key is used for this process. Obtaining the original video is achieved by applying inverse discrete wavelet transform.

A DCT-based robust video steganography method using Bose–Chaudhuri–Hocquenghem codes (BCH) codes was presented in [19]. The algorithm includes encrypting and encoding the information using BCH method. The encoded data were hidden in each Y, U and V planes excluding the DC coefficients of the Discrete Cosine Transform (DCT) coefficients of video frames. Experimental results show that the algorithm can work on both slow and fast video.

In [20], a 2D-DCT of video is used to embed the information by checking DCT coefficients of the video frame.

In [21], LSB replacement technique is used to hide the secret message, and the embedding the message into the video frames. To increase the security of the algorithm, a randomized pixel positions was used to embed the secret data, which is performed by finding an indexed based chaotic sequence and then using this sequence to arrange the pixel position. This work is considered as the soul of this research of hiding text into a sequence of frames. The novelty is to encrypt the text before starting the sending process.

From the literature, hiding text into several images while keeping it invariant to video compression promotes a challenging research. The embedded text also should be encrypted based on complex equations that make it difficult to be resolved in case of detection from unauthorised users.

## 3. THE PROPOSED METHODOLOGY

Section 2 illustrates several researches work in the field of steganography and watermarking. The design of the proposed approach presented in this paper starting from input text and video, producing cypher text, selecting key frames and embedding the cypher text is shown in Figure 1.

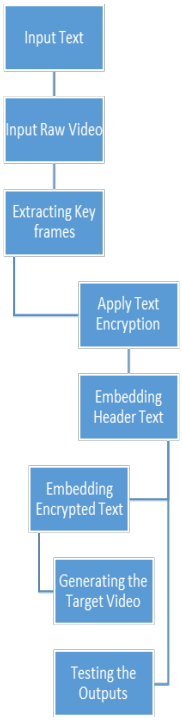



*Figure 1: The Structure Of The Proposed Work.*

The presented work can be divided into five steps; section 3.1 shows the method of extracting the target frames from a video. Encrypting text using a novel technique is introduces in section 3.2. Selecting the required amount of frames to embed the encrypted text is explained in section 3.3 Section 0 explains the method, which will extract the embedded encrypted text. Finally, in section 3.4, the original text can be obtained by reversing the proposed encryption method.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

### 3.1 Frames Extraction

The series of digital frames that are displayed in rapid succession is called digital video. The digital frames (images) represent the motions in the video. In this research, a set of frames is created to embed the required text. The set of frames is used to increase the security level of the hidden text. The frames are selected based on a formula shown in Equation 1. In order to get positive and integer values; the counter index is switched to start from 4 and include all even numbers till N. The target frames based on the index is shown in Table 1. The input text is divided on segments. By supposing the video comprises M frames then the maximum segments number must be less than d(M).

The proposed text encryption method that is described at the next section is based on dividing each segment into 128 bits (16 bytes). Hence the index will be started from 4 and terminates when the mod of dividing the (M) on 16 becomes zero and in this case, we call it (n).

$$d(n) = 0.5n^2 - 1. \quad (1)$$

*Table 1: Frames Selection*

| I (4..n) | Substitute | Target Frames |
|---|---|---|
| 4 | d(4) = 0.5(42) − 1.5(4) | 2 |
| 6 | d(6) = 0.5(62) − 1.5(6) | 9 |
| 8 | d(8) = 0.5(82) − 1.5(8) | 20 |
| 10 | d(10) = 0.5(102) − 1.5(10) | 35 |
| n | d(n) = 0.5n2 − 1.5n | N |

### 3.2 Text Encryption

Before embedding the characters of the text in the extracted frames, it is required to be encrypted. Each segment will be sent as a parameter to the proposed method and returns as an encrypted segment.

1. Accepts the input text segment of size 128 bits.
2. Divide the input segment into two parts (64 bit for each) namely Left Plain Text (LPT) and Right Plain Text (RLT).
3. Divide the LPT into 4 blocks call them B1, B2, B3, and B4.
4. Divide each block into two tokens (8 bits for each) and call each token as follows:

   B1 → LB1 and RB1

   B2 → LB2 and RB2

   Bn → LBn and RBn
5. Convert each token into a binary code.
6. Reverse the binary order for each token.
7. For each token in each block swap the bits as follows:

   Encrypted Block [B1] =

   (LB1[8]+LB1[7]+LB1[4]+LB1[3] ||

   RB1[8]+RB1[7]+RB1[4]+RB1[3] ||

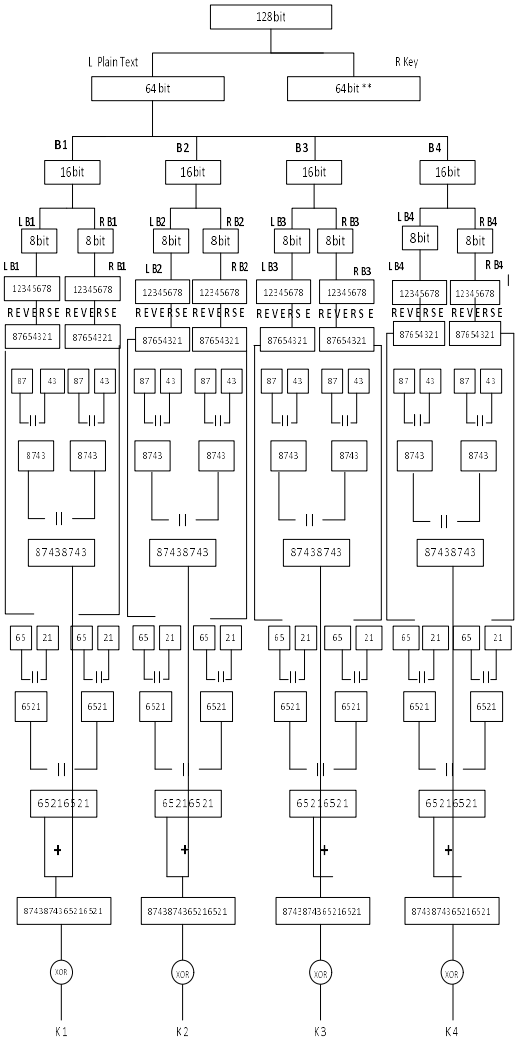
   LB1[6]+LB1[5]+LB1[2]+LB1[1] ||

   RB1[6]+RB1[5]+RB1[2]+RB1[1])
8. Generate 4 keys from the RPT (main key) of size 64 bits as shown in Figure 3, apply the following:
   a. Divide it into 4 blocks (16 bits for each)
   b. Divide each block into 2 tokens (L & R)
   c. Apply left logical shift by 2 bits for each token
   d. Concatenate the L & R token for each block. This must generate 4 keys for each RPT.
9. Apply XOR bitwise LB1 and a random key which has been generated in step 8.d; ( as shown in Figure 4).
10. Save all the selected process in a log file which represents the private key.

Journal of Theoretical and Applied Information Technology
30th June 2019. Vol.97. No 12

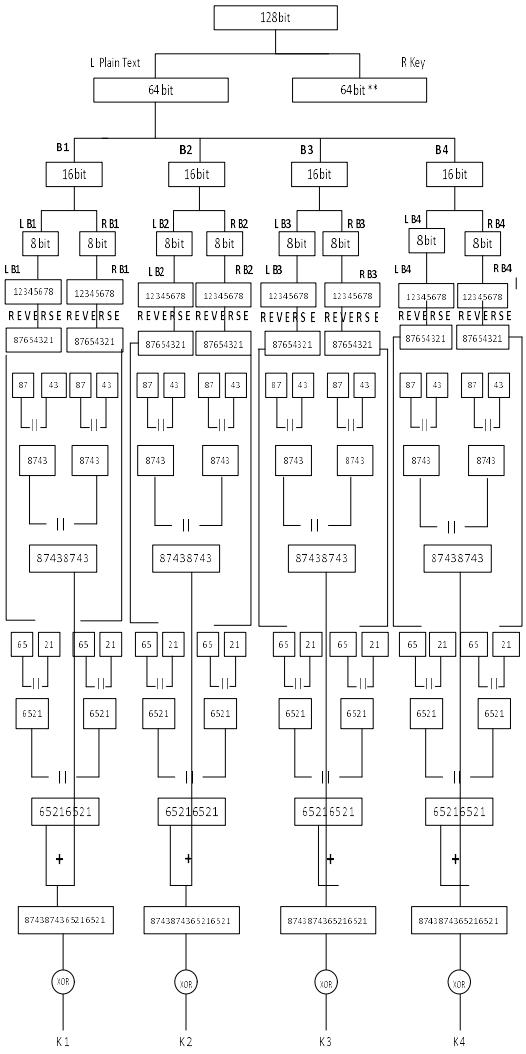
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The whole encryption process is illustrated in Figure 2 below.




Note :
| | : Concatenation
+ : Add
K1&K2&K3&K4 : Key From Another Page (Key Generation Phase ).

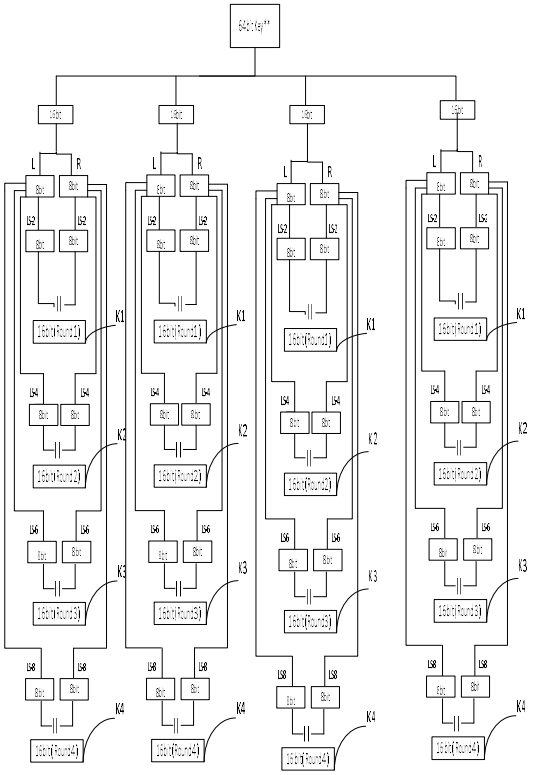
*Figure2 The Proposed Encryption Algorithm*




Note :
| | : Concatenation
+ : Add
K1&K2&K3&K4 : Key From Another Page (Key Generation Phase ).

*Figure 3: The Process Of Generating Cypher Text.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



Note:
||:Concatenation

*Figure 4: Key Creation.*

### 3.3 Text Embedding in Frames

After applying the proposed encryption method, the encrypted text needs to be embedded in the target frames. The locations in each frames should be highly investigated in order to save the text in invariant areas subject to illumination changes or/and video format conversion. The detector of SURF (Speeded Up Robust Features) method which was provided by [22] is used to select the positions of the inserted bits. . This detector concerns with less uniform data that is expected to be less affected. This method doesn't use colour and it returns the positions in the image that are invariant to image multi-scales and illumination changes. These areas are expected to return unique locations which will not be easy to guess. The involved areas are selected at distinctive locations in the image using a Fast Hessian detector. Based on our experiments; the threshold value of 0.7 was founded to get the best result. The keys are saved in the first retrieved area from the first index frame (see equation 1).

### 3.4 Text Extraction & Decryption

This process requires the private keys in order to retrieve the embedded text from all target frames. After applying the equation 1, the keys can be founded in the first frame. Consequently, the Fast Hessian detector is applied on the first frame in order to obtain the keys. Finally, the keys can be used to reverse the processes and getting the original text.

## 4. EXPERIMENTAL RESULTS

The experiments were conducted based on Seaport Security Communication System. The proposed method was tested on a seaport image as shown in figure 5. This image was selected based on its sensitivity to data insertion. The quality of this image is about 75% which is common in use as a default value in many related works.

*Figure 5: The Original Image That Was Used For The Experiments.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

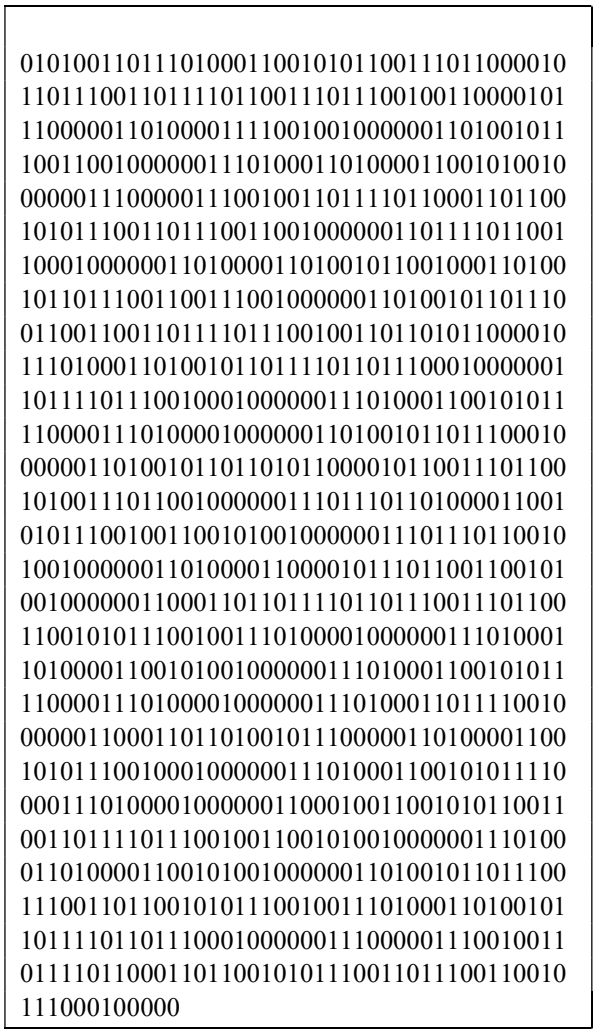

0101001101110100011001010110011101100001
0111100110111101100111011100100110000101
1100000110100001111001001000000110100101
1001100100000011101000110100001100101001
0000011100000111001001101111011000110110
1010111001101110011001000000110111011001
1000100000011010000110100101100100011010
1011011100110011100100000011010010110111
0110011001101111011100100110110101100001
1110100011010010110111101101110001000000
1011110111001000100000011101000110010101
1100001110100001000000011010010111001000
0000011010010110110101100001011001110110
1010011101100100000011101110110100001100
0101110010011001010010000001110111010010
1001000000110100001100001011101100110010
0010000001100011011011110111001110110100
1100101011100100111010000100000011101000
1010000110010100100000011101000110010101
1100001110100001000000011101000110111100
0000011000110110100101110000011010000110
1010111001000100000011101000110010101110
0001110100001000000110001001100101011001
0011011110111001001100101001000000111010
0110100001100101001000000110100101101110
1110011011001010111001001110100011010010
1011110110111000100000011100000111001001
0111101100011011001010111001101110011001
111000100000

Figure 6: Bits Sequence Of The Original Text.

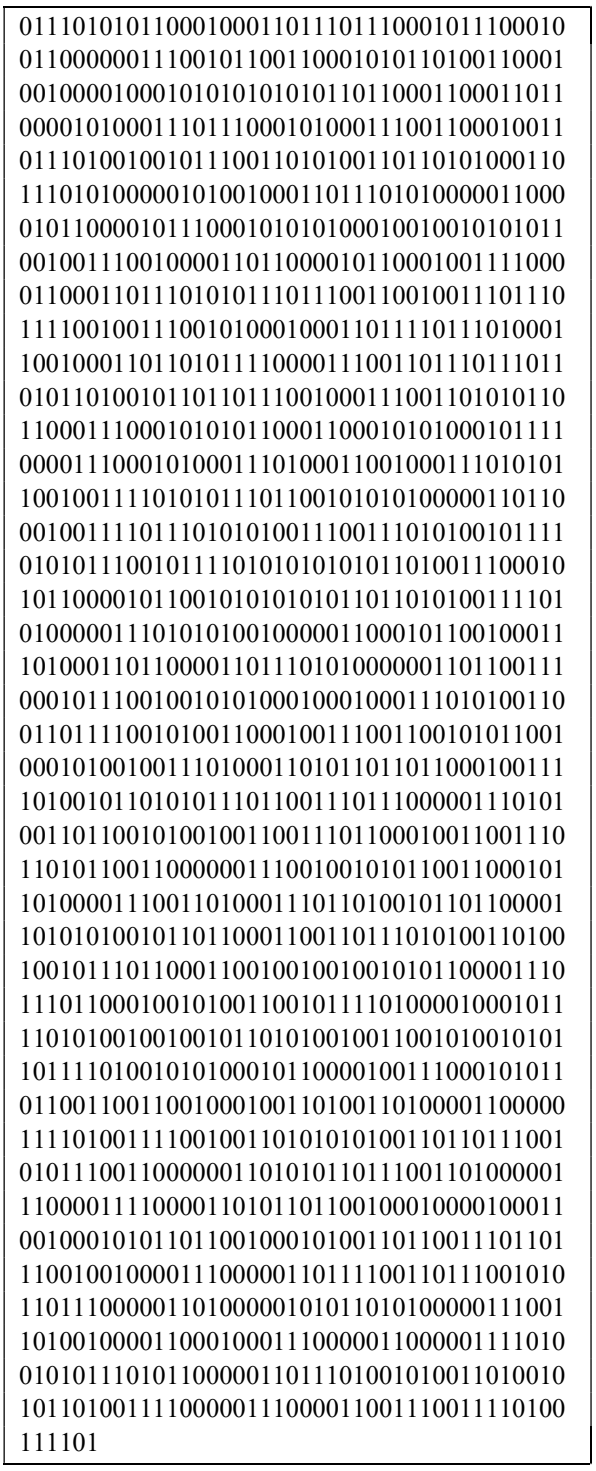

0111010101100010001101110111000101110001
0110000001110010110011000101011010011000
1
0010000100010101010101011011000110001101
1
0000101000111011100010100011100110001001
1
0111010010010111001101010011011010100011
0
1110101000001010010001101110101000001100
0
0101100001011100010101010001001001010101
1
0010011100100001101100001011000100111000
0
0110001101110101011101110011001001110111
0
1111001001110010100010001101111011101000
1
1001000110110101111000011100110111011101
1
0101101001011011011100100011100110101011
0
1100011100010101011000110001010100010111
1
0000111000101000111010001100100011101010
1
1001001111010101110110010101010000011011
0
0010011110111010101001110011101010010111
1
0101011100101111010101010101110100111000
1
0
1011000010110010101010101101110101001111
0
1000000111010101001000001100010110010001
1
1010001101100001101110101000000110110011
1
0001011100100101010001000100011101010011
0
0110111100101001100010011100110010101100
1
0001010010011101000110101101101100010011
1
1010010110101011101100111011100000111010
1
0011011001010010011001110110001001100111
0
1101011001100000011100100101011001100010
1
1010000111001101000111011010010110110000
1
1010101001011011000110011011101010011010
0
1001011101100011001001001001010110000111
0
1110110001001010011001011110100001000101
1
1101010010010010110101001001100101001010
1
1011110100101010001011000010011100010101
1
0110011001100100010011010011010000110000
0
1111010011110010011010101010011011011100
1
0101110011000000110101011011100110100000
1
1100001111000011010110110010001000010001
1
0010001010110110010001010011011001110110
1
1100100100001110000011011110011011100101
0
1101110000011010000010101101010000011100
1
1010010000110001000111000001100000111101
0
0101011101011000001101110100101001101001
0
1011010011110000011100001100111001111010
0
111101

Figure 7: The Binary Bits Of The Ciphertext.

The bits of the original image are shown in figure 6; while the bits sequence for the statement is embedded in the image. The text then is encrypted (ciphertext) before the insertion process as shown

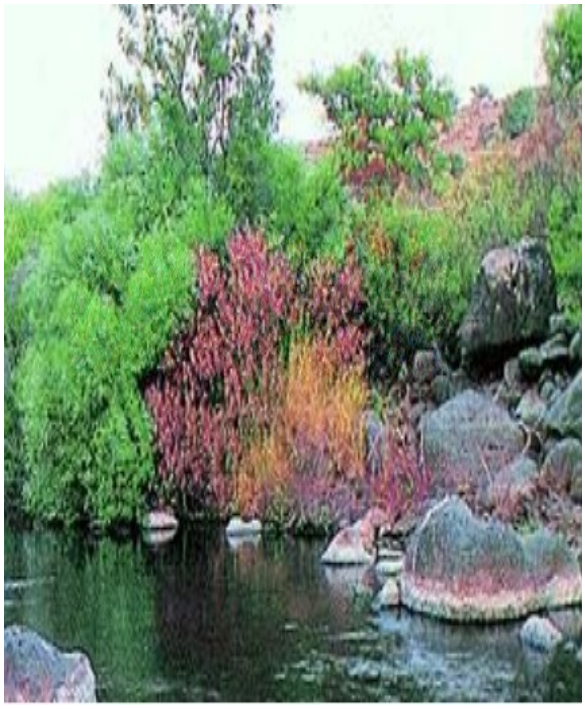
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in Figure 6 while its ciphertext that was inserted into the original image is shown in figure 8.

```
ub7qq09f+LHEUlcaGqG17IsSj7PR7PaaqTIVNCa
bxcuw2wy9DotdmxswkKnG5lqV1QxqGFGVOWe
PlOuNu/W/UZqXYUmOPuH1dtl7P6qrTDu3yLNe
dRtklOKWgpu6Rgbgk09+1hsGil5Kc7SIv2IXwbS/
B/RKRe+zTXN+fdM40zy5SnW05nh8xkdB2+dSg
nHpo7+ph+PsHb80zWX7JiZx8g==
```

*Figure 8: The Generated Ciphertext From The Original Text Shown In The Previous Figure.*

After applying the proposed method for generating the ciphertext; the insertion process were applied on four types of experiments using 1 bit, 2 bits, 4 bits and 8 bits as shown in Figure 9 (a,b,c and d) respectively. The first region returned by the Fast Hessian Detector was used as the starting point of the insertion process for the sequence of bits. The detector concerns with less uniform data that is expected to be less affected. The experiments reveal that if more details in the image region exists then harder to notice if something was added or deleted. But if the data is uniform then every addition or deletion will be more noticeable.

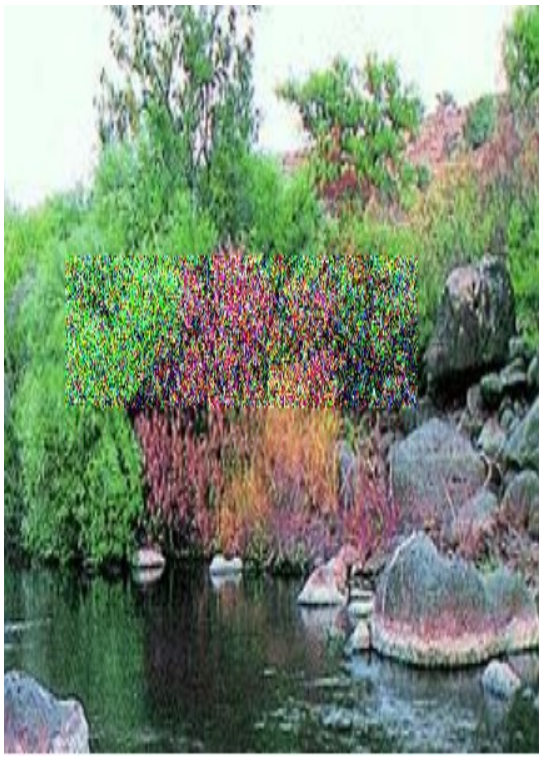


*(a) 1 Bit*

(b) 2 Bits

(c) 4 Bits

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



(d)8 Bits

*Figure 9: The Experimental Results After Inserting The Binary Text Using 1 Bit, 2 Bits, 4 Bits And 8 Bits.*

A video comprising 43 frames recorded by a digital camera with a fame resolution of 800x640` was used to conduct our experiments. In our approach, visually; the best result was achieved by using 2 bits experiment. It should be taken into account that inserting more text in a single image means more noticeable distortions. The message was divided into 4 blocks that equals to the returned number of frames after applying Equation 1. Hence the ciphertext was inserted into frames number 2, 9, 20 and 35. The result was promising with almost no noticeable insertion was detected and the original text was retrieved successfully.

## 5. CONCLUSIONS AND FUTURE WORKS

Hiding information in ways that avoid easy detection of secret text is the core rule of Steganography. While the process of scrambling the text so that it doesn't become understood is called cryptography. In this paper, the text was embedded in selected frames of a video offering a field of growing importance. The novelty of this work is about being able to work with RGB video without considering all frames of the video. However, an equation of a second derivative was used to apply frames selection. Data encryption was applied based on a proposed method that was compared with well-known related works. Prominent results were achieved based on several experiments and evaluations.

Future work can address some of the challenges that still need to be overcome, with suggested solutions and some ideas for further research are to investigate the time required to perform the whole process. In addition, a more complex equation can be built to return more complex set of frames that is not easy to guess.

## ACKNOWLEDGMENT

This research was supported by Al-Ahliyya Amman University and Isra University which are located in Amman, Jordan. We thank our colleagues from both universities who provided insight and expertise that greatly assisted the research.

## REFERENCES:

[1] Lalit Kumar Saini, Vishal Shrivastava, A Survey of Digital Watermarking Techniques and its Applications. Vol. 2. No. 3 P.P.(70-73) , June, 2014.

[2] Doerr, G. and J.-L. Dugelay, A guide tour of video watermarking. Signal processing: Image communication, 2003. 18(4): p. 263-282.

[3] Wu, C.W., G.R. Thompson, and M.J. Stanich. Digital watermarking and steganography via overlays of halftone images. in Mathematics of Data/Image Coding, Compression, and Encryption VII, with Applications. 2004. International Society for Optics and Photonics.

[4] Knox, K.T., Digital watermarking using stochastic screen patterns. 1998, Google Patents.

[5] Shahinfard, E. and S. Kasaei. Digital image watermarking using wavelet transform. in Iranian Conference of Mechatronics Engineering, ICME, Qazvin, Iran. 2003.

[6] Kesidis, A.L. and B. Gatos. A robust image watermarking technique based on spectrum analysis and pseudorandom sequences. in VISAPP (1). 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7] Saboori, A. and S.A. Hosseini. A new method for digital watermarking based on combination of DCT and PCA. in Telecommunications Forum Telfor (TELFOR), 2014 22nd. 2014. IEEE.

[8] Bhaskari, D.L., P. Avadhani, and M. Viswanath, A Layered Approach for Watermarking In Images Based On Huffman Coding. International Journal on Computer Science and Engineering, 2010. 2(02): p. 149-154.

[9] Kostopoulos, H., et al. A Digital Image Watermarking Technique Using Modulated Pascal'S Triangles. in IASTED International Conf. Signal Processing, Pattern Recognition & Applications. 2003.

[10] Pandya, M., H. Joshi, and A. Jani, A novel digital watermarking algorithm using random matrix image. arXiv preprint arXiv:1301.4337, 2013.

[11] Shirali-Shahreza, M.H. and M. Shirali-Shahreza. A new approach to Persian/Arabic text steganography. in Computer and Information Science, 2006 and 2006 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse. ICIS-COMSAR 2006. 5th IEEE/ACIS International Conference on. 2006. IEEE.

[12] Nag, A., et al., A novel technique for image steganography based on Block-DCT and Huffman Encoding. arXiv preprint arXiv:1006.1186, 2010.

[13] Parvez, M.T. and A.A.-A. Gutub. RGB intensity based variable-bits image steganography. in Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE. 2008. IEEE.

[14] Patel, K., et al. Lazy wavelet transform based steganography in video. in Communication Systems and Network Technologies (CSNT), 2013 International Conference on. 2013. IEEE.

[15] Patel, R. and M. Patel. Steganography over video file by hiding video in another video file, random byte hiding and LSB technique. in Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. 2014. IEEE.

[16] Kar, N., K. Mandal, and B. Bhattacharya, Improved chaos-based video steganography using DNA alphabets. ICT Express, 2018. 4(1): p. 6-13.

[17] Bhole, A.T. and R. Patel. Steganography over video file using Random Byte Hiding and LSB technique. in Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on. 2012. IEEE.

[18] Dumitrescu, S., X. Wu, and Z. Wang, Detection of LSB steganography via sample pair analysis. IEEE transactions on Signal Processing, 2003. 51(7): p. 1995-2007.

[19] Thakur, A., H. Singh, and S. Sharda, Secure Video Steganography based on Discrete Wavelet Transform and Arnold Transform. International Journal of Computer Applications, 2015. 123(11).

[20] Mstafa, R.J. and K.M. Elleithy. A DCT-based robust video steganographic method using BCH error correcting codes. in Systems, Applications and Technology Conference (LISAT), 2016 IEEE Long Island. 2016. IEEE.

[21] Rajesh, G. and A.S. Nargunam, Steganography algorithm based on discrete cosine transform for data embedding into raw video streams. 2013.

[22] Bay, H., T. Tuytelaars, and L. Van Gool. Surf: Speeded up robust features. in European conference on computer vision. 2006. Springer.