ISSN (e): 2250 – 3005 || Volume, 09 || Issue, 1 || January – 2019 ||
International Journal of Computational Engineering Research (IJCER)

Embedding Encrypted Image within Video for Secure Transmission

Dhiman Karmakar[1]
1 Assistant Professor, Computer Science, Surendranath College, Kolkata,
Corresponding Author: Dhiman Karmakar

ABSTRACT:
Different techniques are available for image cryptography and image steganography. This paper proposes a scheme for embedding an image within a video, so that, the perceived quality of the video seems to be unaffected. The secret image is encrypted before embedding in the video. A decryption technique is used to retrieve the original image, in the receiver side. Here, emphasis is imposed on the methodology of embedding the image, rather than on the encryption algorithm used. The image is divided into n subparts or shares for a video consisting of more than n frames. Each of these image-shares is first encrypted and then appended with each video frame, before transit. On recipient's end, the received video is broken down into frames; image share from each of the video frame is extracted and deciphered.
KEYWORDS: *Cryptography, Steganography, Watermarking, Data-hiding, Plaintext, Ciphertext, image, video*

Date of Submission: 03-02-2019 Date of acceptance: 20-02-2019

I. INTRODUCTION

There emerges a need for secured transmission of data, with the rapid growth of multimedia and digital communication in recent times. An attacker (intruder) with malicious intention can snatch the data during transmission or intrude into recipient's account or even worse, may change the data in transit and send the corrupted data to the receiver. Thus systems are often get compromised. Cryptography and steganography are the tools to combat against such threats. In cryptography, sender sends the cipher-text CT (encrypted form of plain-text PT i.e. the intended text to be sent) to the receiver and using a decryption process upon CT, the receiver deciphers the CT to obtain the PT. Note that, any cipher-text being a meaningless stream of symbols and characters arouses hacker's suspicion and attention to much extent. Stegangraphy on the other hand, deceive the intruder by embedding PT carefully within a meaningful text, image, video or signal, so that, the overall perceptual appearance of the resulting media remains unaltered. Intruder may pretend the transmission of video or signal, whereas originally PT is being conveyed.

A distinction between steganography and cryptography and the limitations of the duo is well illustrated in [1]. This difference is also depicted in [2] where a random phase mask encoding is developed, in frequency domain. Fonteneau et. al [3] proposes embedding of a hierarchically selected encryption service, within a multi-resolution lossless codec. There are several methods of image encryption and yet the new techniques are evolving [4]. These techniques are neatly compared and analyzed in [5]. Bhaumik et. al [6] proposes a data hiding technique in high resolution AVI videos. Different tools, like genetic algorithms(GA), is used in the field of image encryption [7].An interesting work by Jackson et. al [8] also uses GA to develop a CIS (Computational Immune System) classifier to differentiate a clear image from a stego (resulting image containing the hidden information) image. Watermarking is a thrust area for image or video copyright protection. Naor et. al [9] introduced the concept of visual cryptography in this arena. A simple watermarking method on color images can be observed in [10].

Lenka et al [11] implements a novel steganography approach with the help of LSB array. After image binarization four LSB arrays are utilized. One array among them is formed using the secret data size. Secret data is embedded in one of the particular region of that array. An interesting article by Jain et al [12] depicts a procedure of hiding sensitive medical records like HIV reports, baby girl fetus, and patient's identity information within their Brain disease medical image files,like scan image or MRI image. They have proposed a technique of diagonal queue least significant bit substitution. Singla et al[13] proposed a steganographic method using LSB and DCT for hiding data. Here each bit of the secret data is embedded altering the LSB. A step by

step journey in the field of video steganography along with a comparative study between the different methodologies can be observed in [14].
This paper shows a technique where an image S, to be sent, is encrypted and embedded within a video V_0, so that, the intruder pretends only the existence of resulting video V_1 and has no idea on the transmission of S. The intruder may consider the existence of S, if at all visible, as a noise of V_1.

II. PROPOSED METHOD OF IMAGE EMBEDDING

The image embedding algorithm hides the image within a video. Different parts of the image are encrypted and embedded in each of the video frame.

2.1. Image embedding algorithm

Algorithm 1: Image Embedding in Video
1: Extract T number of frames F_1 , F_2,…, F_T , each of size pX q, from the color video V_0 //We assume q > n and T > m
2: **for** i ← 1 to m **do** // modify ROW^{th} row of the frames
3: $F_i(ROW, col)$← encrypt(S(i, col)), for all columns col ranging from 1 to n
4: **end for**
5: Frames F_{m+1}, F_{m+2},…,F_T remains unchanged.
6: Construct video V_1 from frames F_1, F_2,…,F_T .
7: Send the video V_1

2.2. Illustration

The first algorithm depicts how the image S of size mXn, to be conveyed, is appended in a video. At first the given video V_0 is divided into T number of frames, namely F_1, F_2 to F_T. We assume that the frame dimension is pXq. The image S is divided into m number of image strips, each of unit height and width n. Each of these strips is encrypted, such that its width n does not alter. Note that, the method of encryption is not our area of concern. Couple of things to be remembered during the encryption process. Firstly, strip width should remain the same in each frame and secondly the cipher text, like plain text, should consists of integers only. It ensures, that the strip ever appended to an image (here, video frame), does not create any problem displaying the image. Our intuition is to append the encrypted strip to any particular row ROW of a frame. Therefore, it is trivial, that the frame width q should be no less than the strip width (i.e. q > n). Again, as each strip is to be appended to each frame , number of frames T should be no less than image height m (i.e. T > m).The video V_1 is constructed from these modified frames and sent to recipient. Note that, out of these T frames, first m contains the hidden image strips.
The second algorithm works in receiver end. It divides V_1 into T frames. The particular row ROW, containing hidden image strip, of each of the first m frames, is decrypted and the resulting strip is appended to S, one after another. On completion of
the procedure, S will contain the image sent with the video.

Algorithm 2: Image Extraction from Video
1: Extract T number of frames F_1, F_2,…,F_T , each of size pXq, from the color video V_1
2: **for** i← 1 to m **do** //get hidden values from ROW^{th} row of the frames
3: S(i; col) ← decrypt(Fi(ROW; col)), for all columns col ranging from 1 to n
4: **end for**
5: view S

III. EXPERIMENTAL RESULT ANALYSIS

Our experiment including construction of video and selection of secret image etc is carried out using [15]. A snapshot of a particular (say, k^{th}) video frame, in which the experiment is carried out, is depicted in Fig.1(a). Fig.1(b) shows the k^{th} frame, after embedding the image strip to the bottom row. The difference between these two images is not readily recognized by naked eye. However, when the bottom portion of the said images is zoomed, the distinction is visible. We may acknowledge, that, there is a very thin information strip attached to Fig.1(d); but the same is absent in Fig.1(c).
Fig.2 illustrates a midway of the ongoing decryption phase (algorithm 2), where first k rows (Hence, first k frames of V_1) of S, have been successfully decrypted and appended. The black portion of the image, should start from k + 1^{th} row of S and is yet to
be processed.

1. (a) Original Video frame snapshot

1. (b) Frame with embedded image share

1. (c) zoomed bottom portion of (a)

1. (d) zoomed bottom portion of (b)

Figure 1. Embedding image within video

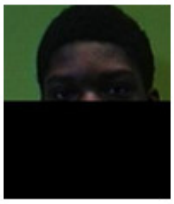

Figure 2. Retrieval process of the hidden image from the video

IV. LIMITATIONS AND FUTURE SCOPE

The overall system can be improved to work in a real time scenario. That is, hidden image strip in each frame, is decrypted and displayed, as and when a particular frame reaches the recipient.

Instead of hiding the image, within the source video V_s, a hidden video V_h, can be embedded within V_s, where size of V_h must be much less than that of V_s. Please note that, much larger size of the sent video, with respect to the image size, is a limitation of our method.

Our algorithm does not put any emphasis on the encryption method used upon the gray level values of the image. In a larger screen, bottom image strip, embedded in the video frame, becomes more visible and hence invites suspicion to intruder's mind. He could separate the bottom strips from video and start permuting those strips to reach the hidden image. However, if the strips represent ciphertexts, task for the intruders becomes immensely tedious. On completion of the permutation procedure, there can be an automated meaningful-image detection scheme. Otherwise, manual detection of a meaningful image from a large repository of permutation-generated images could be extremely time-consuming. Assuming T >> m (see the algorithms), we may generate T - m number of noise-image strips and embed them to rest of the T - m video frames. It ensures, further difficulty, in terms of automatically determining meaningful image from permutation generated image set I, as the number of images in I i.e.| I |, drastically increases, with the inclusion of noise strips, from m! to T!.

Since, gray values need to be integers, ciphertext, being represented as an image strip, must be kept integers, within a specific range. This constraint should be kept in mind, while designing the encryption scheme. Here, we use simple exclusive-OR (on gray values) symmetric key encryption technique. However, a chain of different encryption methods, following a particular sequence can be used on the source image, before embedding it to video and exactly a reverse sequence of such methods can be applied in recipient's end, for decryption. In a more advanced stage, this ordering of encryption methods can be changed in random. Our method is basically a combination of cryptography and steganography on images. Here, use of steganography carries more importance as the overall method can be performed correctly, without incorporating any encryption-decryption scheme. The gray values (hidden message), can be easily scrambled using the aforesaid steganography approach (see algorithms). Future work can be performed imposing equal importance on both the techniques.

REFERENCES

[1]. Ross J. Anderson and Fabien A.P. Petitcolas. On the limits of steganography. IEEE Journal of Selected Areas in Communications, 16(4):474-481, May,1998.

[2]. Zenon Hrytskiv, Sviatoslav Voloshynovskiy, and Yuriy Rytsar. Cryptography and steganography of video information in modern communications.Electronics and Energetics, 1(11):115{125, 1998.

[3]. C. Fonteneau, J. Motsch, M. Babel, and O. Deforges. A hierarchical selective encryption technique in a scalable image codec. International Conference in Communications, Bucharest : Roumanie, 2008.

[4]. A. Mitra, Y. V. Subba Rao, and S. R. M.Prasanna. A new image encryption approach using combinational permutation techniques. International Journal of Computer Science, 1(2):127{131, 2006.

[5]. Ismet ztrk and Ibrahim Sogukpnar. Analysis and comparison of image encryption algorithms. World Academy of Science, Engineering and Technology, 3:26{30, 2005.

[6]. Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas. Data hiding in video. international Journal of Database Theory and Application, 2(2):9{15, June,2009.

[7]. Mohammed A.F. Al-Husainy. Image encryption using genetic algorithm. Information Technology Journal, 5(3):516{519, 2006.

[8]. Jacob T. Jackson, Gregg H. Gunsch, Jr. Roger L. Claypoole, and Gary B. Lamont. Blind steganography detection using a computational immune system: A work in progress. International Journal of Digital Evidence, 1(4), 2003.

[9]. M. Naor and A. Shamir. Visual cryptography Lecture Notes in Computer Science, Springer Verlag, 950:1{12, 1995.

[10]. Rawan I. Zaghloul and Enas F. Al-Rawashdeh. Hsv image watermarking scheme based on visual cryptography. PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY, 34:482-485,Otober,2008.

[11]. Gandharba S, Lenka SK, A novel steganography technique by mapping words with LSB array. Int J Signal Imaging Syst Eng, 2015

[12]. Mamta Jain and Saroj Kumar Lenka, Diagonal queue medical image steganography with Rabin cryptosystem, Brain Informatics, 2016 3:32,2016
[13]. Deepak Singla and Rupali Syal, Data Security Using LSB & DCT Steganography In Images,IJCER, 2(359-364),2012
[14]. S.M.Nasreen,G.Jalewal,S.Sutradhar, A Study on Video Steganographic Techniques, IJCER, 5(29-34),2015
[15]. Libor Spacek's Facial Images Databases; http://cmp.felk.cvut.cz/~spacelib/faces/

Dhiman Karmakar" Embedding Encrypted Image within Video for Secure Transmission" International Journal of Computational Engineering Research (IJCER), vol. 09, no. 1, 2019, pp 65-68