International Research Journal of Advanced Engineering and Science

ISSN: 2455-9024

Conceal Message and Secure Video Transmission

Sree Rag R[1], Prasanth M[2]

[1, 2]Department of ECE, University of Calicut, NCERC, Pampady, Kerala, India-680588

Abstract— *The paper provides a method for communicating the message (text, image and video) secretly using a cover video. This can be achieved by using the combination of both steganography and cryptography. Steganography is the science of hiding information. Cryptography is the study of transform the information in order to make it secure from unintended recipients or use. Here cover video is considered as a sequence of image frames. If message is a video then each secret image frames of the secret video is suitably embedded into image frame of cover video or if the message is a text or image then randomly select a frame of cover video and embedded into it. Here, the bits of the message frame are directly embedded into least significant bit plane of the cover-frame in a certain sequence. Modulating the least significant bit cannot be identified in human perceptible difference because the amplitude of the change is small. Each pixel (8 Bits) is hided in 4 pixels (4*8=32 bits) of video frame (2 bit of message image is substituted in LSB). Finally the resultant video is also encrypted with random key. Based on the user id and password we can extract the video (contain both cover and message video). If the user id and password is correct then by using LSB extraction of the resultant video we will get the message video and by MSB extraction we will get the cover video. If the user id and password is incorrect then the message is deleted from the cover video.*

Keywords— *LSB, MSB, steganography, cryptography*

I. INTRODUCTION

The fast growth of message communication through internet made it easier to send the message faster and accurate to the destination. Internet is a global network for connecting millions of computers around the world. People can easily access to the internet. Therefore in between sender and receiver it may possible by any person to modify and misuse the valuable information. During communication it is important to protect this valuable information from any kind of leakages or illegal access. To avoid such an illegal access this method is used. Steganography and Cryptography are the primary methods for hiding the information and provide security. Cryptography and steganography are often regarded as similar practices, and whilst both fields deal with secure communication. Steganography is the art of covered or hidden writing. The term is derived from two Greek words stegano and graphia, meaning "covered" and "writing" respectively. Put simply, steganography is the procedure of hiding communication in the presence of a message is secret.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. It is the process of enciphering and deciphering of messages in secret code or cipher.

Here cover is a video, therefore we can hide more information and cover video is the medium for messages or information. This video considered as a sequence of image frames. If message is a video then each secret image frames of the secret video is hide into image frame of cover video or if the message is a text or image then select one of the frame of cover video and hide into it.

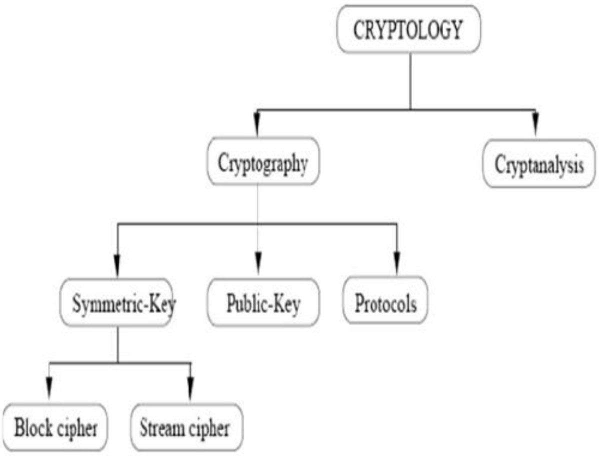


Fig 1. Cryptography.

II. RELATED WORKS

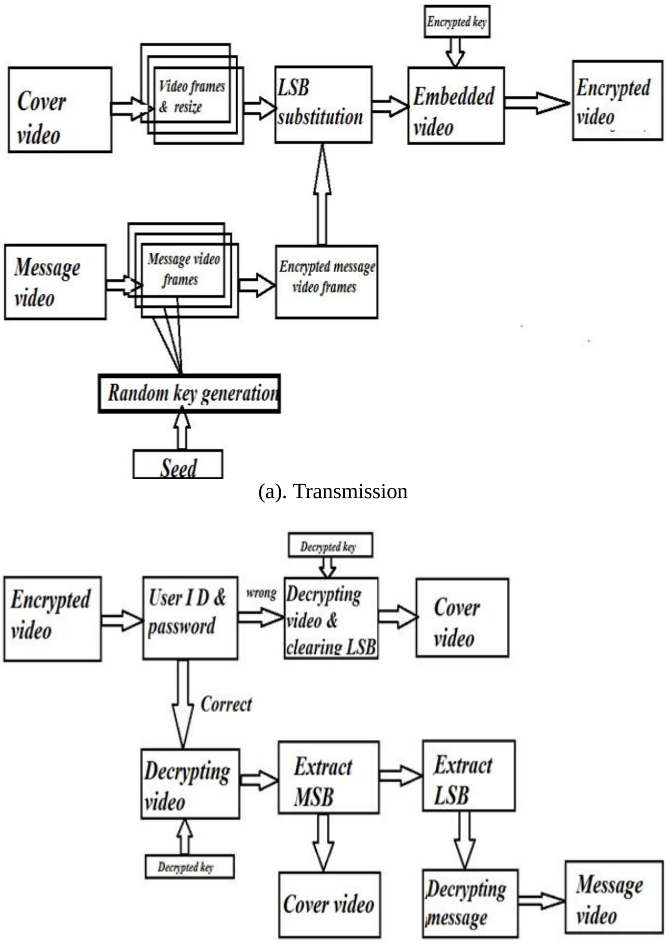
Various modes are proposed for securing image transmission and the two main approaches are data hiding and image encryption. In Image Encryption no one can obtain the secret image from the encrypted image unless who has the not known the secret key. The encrypted image is a meaningless noise file, which cannot provide any information unless it is not decrypted and may arouse an attacker's attention. The remedy to this solution is data hiding that is hides a secret data into a image, no can identify the existence of the secret information. The problem associated with this method is to embed large amount of data into a single image.

Recently a new technique is proposed by Lai and Tsai for secure image transmission, i.e. by using a new type of computer art image called secret fragment visible mosaic image. Mosaic which is generate automatically by composing small fragments of a given image to become a target image in mosaic form and embedding the secret image visibly but secretly in the resulting mosaic image. Here the target image which is required to hide the secret image has to be preselected from a data base. Large database requirement was one of the main weaknesses of this method. That is the user was not admitting to select freely his/her favorite image as target image. To avoid this issue while keeping its merit a new approach was proposed by Ya-Lin Lee and Tsai is design of new method that can convert a secret image into a secret fragment visible mosaic image of the equal size that has a visual appearance of any freely selected target image without the need of a data base. The limitation for this approach is that only image transmission was possible, not the video.

III. PROPOSED SYSTEM

To overcome all the above mentioned issues a new technique is introduced which can be used to transmit video along with hiding information. The main aim of this project is to develop a video steganography system that fully utilizes the features of a video container file. The proposed system should be secure and practical. This system provides a method for communicating the message (text, image and video) secretly using a cover video. This can be achieved by using the combination of both steganography and cryptography. Steganography is the science of hiding information. Cryptography is the study of transform the information in order to make it secure from unintended recipients or use. Here cover video is considered as a sequence of image frames. If message is a video then each secret image frames of the secret video is suitably embedded into image frame of cover video or if the message is a text or image then randomly select a frame of cover video and embedded into it. The resultant video is encrypted. The message is extracted from the resultant encrypted video by using a user name and password. This password is the seed of key generation algorithm In the proposed system there are two cases, (a).the message is a video (b) the message is a image or texture

Case 1: Message is a video



(a). Transmission

(b). Receiving section

Fig. 2. Block diagram of video steganography when message is video.

First a target video is selected arbitrarily, and confirms whether the message is a video. If the message is also a video then separate the message video into sequence of secret image frame. The size of the target video is set to a unique size, with respect to the message video .Take the first message video frame and hides it into the first cover video frame, then take the second message video frame and hide it into the second cover video frame and so on. The resultant video is stored and encrypted. Based on the user id and password extract the video (contain both cover and message video). If the user id and password is correct then by using LSB extraction of the resultant video we will get the message video and by MSB extraction we will get the cover video. If the user id and password is incorrect then the message is deleted from the cover video.

Case 2: *Message is a image or text*

If the message is a image or text, then select a cover video is selected arbitrarily, and confirms whether the message is a video. Choose one of the image frames of the cover video. The size of the cover video is set to a unique size, with respect to the message. In the selected cover video frame hide the image or text. The resultant video is stored and encrypted by stream cipher encryption. Based on the user and id and password we can provide decryption algorithm we and extract the video (contain both cover and message video). By using blind detection algorithm, we will get the message image or text

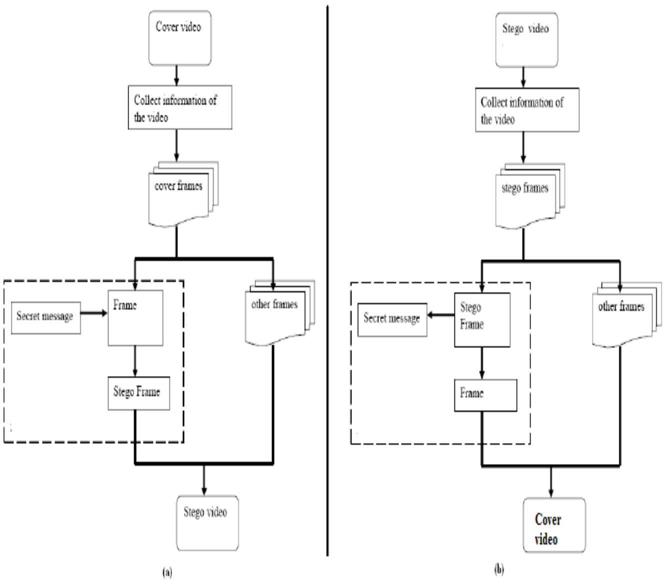


Fig. 3. Block diagram of video steganography when message is image or text.

IV. LEAST SIGNIFICANT BIT

This method is the more popular one among hiding images. Programs that use the Least Significant Bit, or LSB, method hide the message in the least significant bit of every byte in an image. While doing this the value of each pixel changed then also there is not enough to make significant changes to the image. For example a 24-bit image, 3 bytes are used for each pixel, so each pixel could hide 3 bits of a secret message. The altered image would look identical to the human eye, even when compared to the original. Ann example shown below

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

If the binary representation of 200 is 11001001, is embedded into the least significant bits of the cover image, then resulting binary representation is
(0010110**1** 0001110**1** 1101110**0**)
(1010011**0** 1100010**1** 0000110**0**)
(1101001**0** 1010110**0** 0110001**1**)

The three bit in bold are underlined bits needed to be changed according to the embedded message .White Noise Storm and S-Tools were mostly using commercial programs in LSB encoding

A. *Algorithm steps for LSB Technique*

Each pixel (8 Bits) is hided in 4 pixels (4*8=32 bits) of video frame (2 bit of message image is substituted in LSB). If message size is m1*n1 and cover frame size if m2*n2 Then number of pixels in one row of 1 frame that can be hided are given by Y=n2/8 pixels. Consider the message frame is 8 bit (D7 D6 D5 D4 D3 D2 D1 D0).

Step 1: Choose the cover video(C) and message video (M) or image. The size of message video frame is m1*n1 and for cover video frame is m2*n2.
Step 2: The size of cover video frame is resized to 2m1*2n2.
Step 3: Convert the cover image frame ‘C’ into unsigned integer format (uint8) and clear the 2 bit in LSB (i.e. multiply it with 252)
Step 4: The message frame M is stored in another variable called y1. The MSB of y1 is shifted to the LSB side and stored in another variable called y1_.(0000D7D6D5D4).
Step 5: Again a 2 bit left shift is applied to y1_. Now y1_ contain D7 and D6 bit only in the LSB side.
Step 6: A ‘bit and’ operation is applied between y1 and 3. Now y1 contain D5 and D4 bit only in the LSB side.
Step 7: A bit and operation is applied between M and 12. The result is stored in yLSB1. A 2 bit shift is again applied to yLSB1. Now it contains D3 and D2 bit only in the LSB side.
Step 8: A bit and operation is applied between M and 3. The result is stored in yLSB2. Now it contains D1 and D0 bit only in the LSB side.
Step 9: All D7 and D6 bit of message frame is stored in the LSB side of first quadrant of C.
Step 10: All D3 and D2 bit of message frame is stored in the LSB side of second quadrant of C.
Step 11: All D1 and D0 bit of message frame is stored in the LSB side of third quadrant of C.
Step 12: All D4 and D3 bit of message frame is stored in the LSB side of fourth quadrant of C.

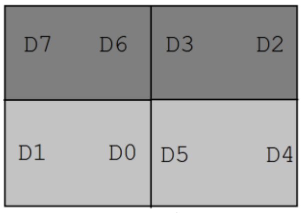


Fig. 4. Block diagram of LSB substitution.

V. Stream Cipher Encryption

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (key stream). In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the key stream, to give a digit of the cipher text stream. Since encryption of each digit is dependent on the current state of the cipher, so it is also known as state cipher. In practice, a digit is typically a bit and the combining operation an exclusive-or (XOR). The pseudorandom key stream is typically generated serially from a random seed value using digital shift registers. The seed value serves as the cryptographic key for decrypting the cipher text stream. Stream ciphers represent a different approach to symmetric encryption from block ciphers. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation. This distinction is not always clear-cut: in some modes of operation, a block cipher primitive is used in such a way that it acts effectively as a stream cipher. Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity.

A. *Stream Cipher Algorithm*

Step 1: Choose the video which is to be encrypted.
Step 2: Calculate the video column length and breadth and it is stored in x and y respectively.
Step 3: Generate different key stream for each frame in a video by using key generation algorithm.
Step 4: Divide the color frame into Red (R), Green (G) and Blue (B) components. And first take the Red component
Step 5: Encrypt the entire length and breadth of the image frame by using the random key in the below formula.
Encrypted Image (L,B, color comp)=BITOR (image frame(L,B, color comp), Fkey(L,B,1)))
If Color map=3 then go to step 8.
Step 6: Then take second color component Green and go to step 5.
Step 7: Then take third color component blue and go to step 5.
Step 8: Fully encrypted video is stored
Step 9: End

B. *Key Generation Algorithm*

Step 1: Calculate the video column length and breadth and it is stored in x and y respectively.
Step 2: Compute p=x*y. and r=p*8
Step 3: Provide a seed value s.
Step 4: Find value for every J. J is varies from 1 to r.
K(J)= 1 - 2* s *s;
Step 5: Create an array KEY with length p with initial value zero.
Step 6: Find value for every J. Initially J =1 and incremented by one in next step.
Step 7: Initially I =1 and incremented by one in next step.

KEY(J) = KEY(J) + key(I*J)* 2 ^ (I-1)

Step 8: If I=8 go to step 6.
Step 7: If J = p then go to step 8 otherwise go to step 6.
Step 8: End.

VI. BLIND DETECTION ALGORITHM

Blind detection is the extraction process. Blind signal separation, also known as blind source separation, is the separation of a set of source signals from a set of mixed signals, without the aid of information (or with very little information) about the source signals. Steganalysis is the study of detecting messages hidden using steganography

Step 1: Load cipher video.

Step 2: Calculate the length and breadth of cipher video and reduced to half its size then stored in variable x and y respectively..

Step 3: From the first quadrant extract all the 2 bit LSB by using 'bit shift' and 'bit and' operation. Therefore we can obtain the D7 and D6 bits.

Step 4: From the second quadrant extract all the 2 bit LSB by using 'bit shift' and 'bit and' operation. Therefore we can obtain the D3 and D2 bits.

Step 5: From the third quadrant extract all the 2 bit LSB by using 'bit shift' and 'bit and' operation. Therefore we can obtain the D1 and D0 bits.

Step 6: From the fourth quadrant extract all the 2 bit LSB by using 'bit shift' and 'bit and' operation. Therefore we can obtain the D4 and D3 bits.

Step 7: All these bits are arranged in the specified manner using 'shift' and 'and' operation in order to obtain the exact message.

Step 8: End.

VII. SIMULATION RESULTS

Experimental results has been shown in this section, all the experiments have been done in MATLAB 2013a. We had tested the proposed algorithm for various images and videos in the same cover video and compare the MSE and PSNR value.

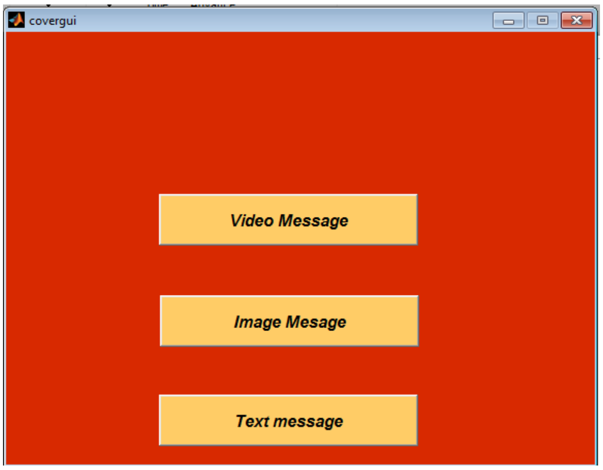


Fig. 5. Opening GUI.

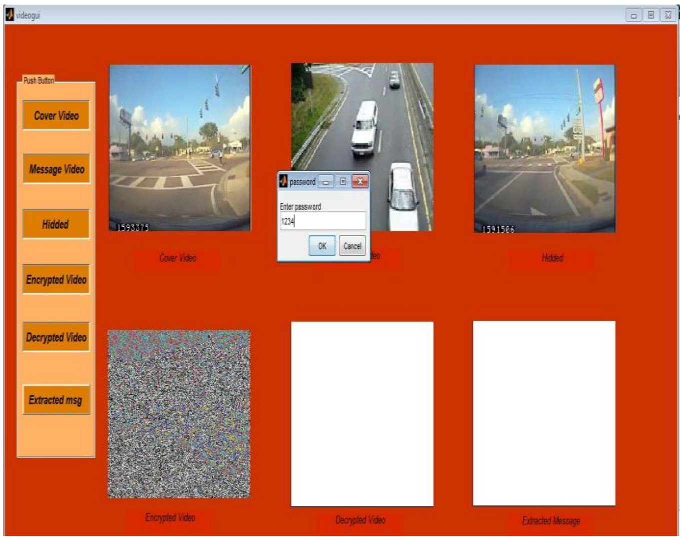


Fig. 6. Password added video GUI.

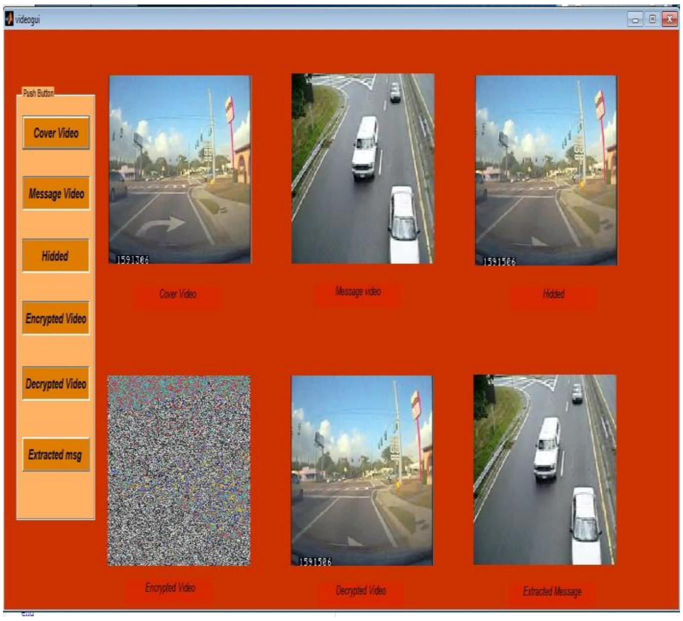


Fig. 7. Video GUI.

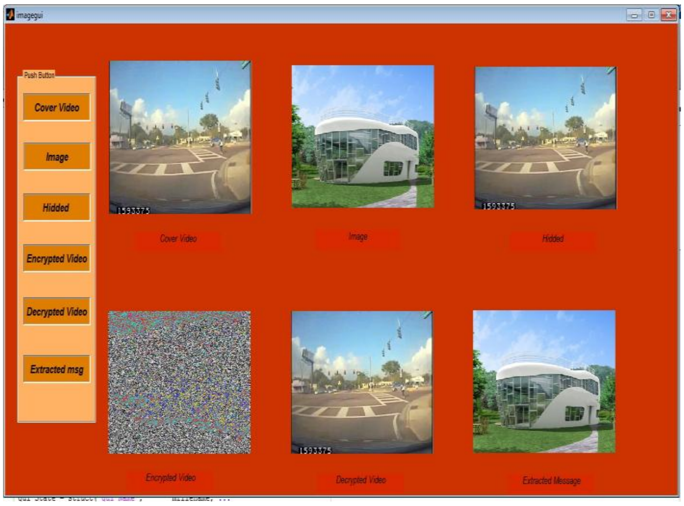
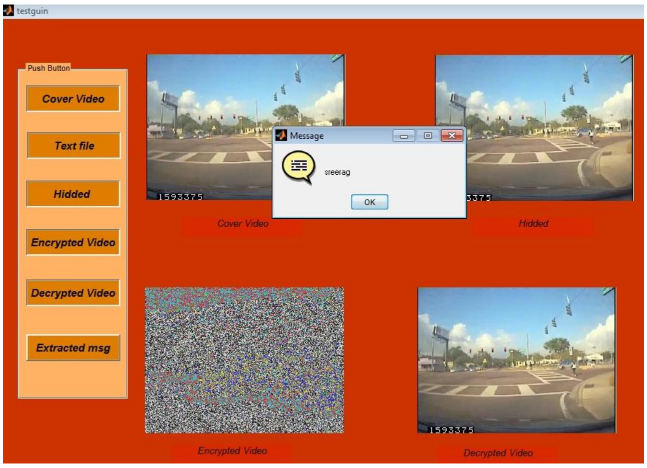


Fig. 8. Image GUI.

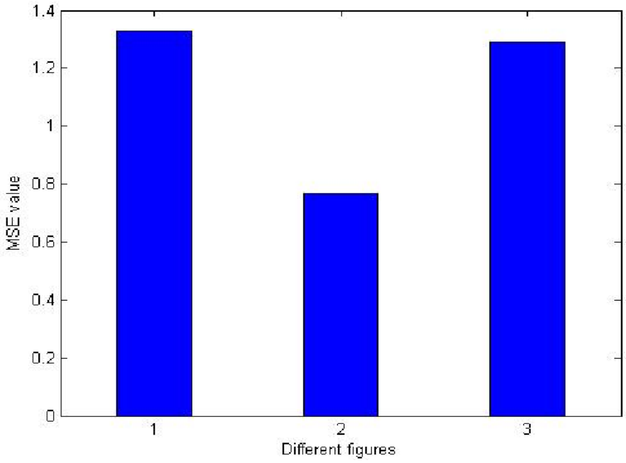


Message

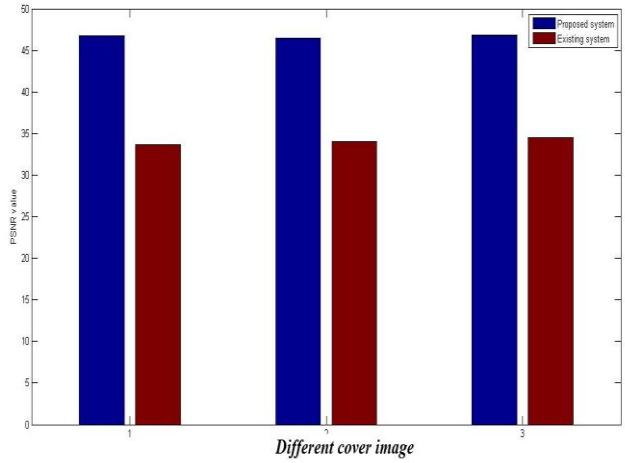
sreerag

OK

Fig. 9. Text message GUI.



(a)



(b)

Fig. 10. (a) MSE value of proposed system, (b) PSNR value of proposed system for different cover image.

VIII. Conclusion

The intension of this project is to provide a protection on data during transmission. The important features of the proposed system is it plays a vital role in transmitting the information mapped on an either video or a image file very effectively and efficiently. The message either image or a video is not visible to the naked eye when we embed the message information into the LSB side of cover image. By using the private key and certain algorithm (LSB, encryption, decryption) only can decode and identify the original information into its original form. The Implementation is simple and also provides security. With the use of the cryptography and steganography combination the information security can be increased.

References

[1] A. C. Bovik, *Handbook of Image and Video Processing*, Elsevier Inc., ISBN 0-12- 119192-1.

[2] A. Murat Tekalp, *Digital Video Processing*, Prentice Hall Signal Processing Series.

[3] R. Schaphorst, *Videoconferencing and Video Telephony*, Boston, MA: Artech House Publishers, 1996.

[4] Adnan M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147–1156, 2004.

[5] Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Transactions on Image Processing*, vol. 12, issue 2, pp. 221- 229, 2003.

[6] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," *IEEE Transactions on Multimedia*, vol. 14, no. 3, pp. 703–716, 2012.

[7] B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," *Information Sciences*, vol. 180, no. 23, pp. 4672–4684, 2010.

[8] W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Letters*, vol. 19, no. 4, pp. 199–202, 2012.

[9] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions On Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[10] N. Keshaveni, S. Ramachandran, and K. S. Gurumurthy, "Implementation of context adaptive variable length coder for H.264 video encoder," *International Journal of Recent Trends in Engineering*, vol. 2, no. 5, pp. 341-345, 2009.

[11] B. Raja Rao, P. A. Kumar, M. Nagu, and K. R. Mohana Rao, "A novel information security scheme using cryptic steganography," *Indian Journal of Computer Science and Engineering*, vol. 1 no. 4, pp. 327-332

[12] D. Wagner and A. Roos, "Class of weak keys in the RC4 stream cipher," Two posts in sci.crypt, 1995.

[13] Grosul and D. Wallach, "A related key cryptanalysis of RC4," Tech. Report TR-00-358, Department of Computer Science, Rice University, 2000.

[14] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the scheduling algorithm of RC4," *Selected Areas in Cryptography, Lecture Notes in Computer Science*, Springer, Berlin, vol. 2259, pp. 1-24, 2001.

[15] Mantin, "Analysis of the stream cipher RC4," Master's Thesis, The Weizmann Institute of Science, 2001.

[16] H. Wu, "The Stream Cipher HC-128," New Stream Cipher Designs - The eSTREAM Finalists, LNCS 4986, Springer-Verlag, 2008.

[17] Y. Liu and T. Qin, "The key and IV setup of the stream ciphers HC-256 and HC-128," *International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 2, pp. 430–433, 2009.

[18] W. Stallings, *Cryptography and Network Security*, Pearson Education International, 2003

[19] S. Priya, and A. Amsaveni, "Edge adaptive image steganography in DWT Domain," *International Journal of Advances in Image Processing*, vol. 2, pp. 91-94, 2012.

[20] A. Pradhan, D. Sharma, G. Swain, "Variable rate steganography in digital images using two, three and four neighbor pixels," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 3, no. 3, pp. 457-463, 2012.