Survey on an Efficient Video Steganography Using RSA and Modified OPAP

Ram Chandra Patnaik, Himani Agrawal

Abstract— **This paper proposed An Efficient Video Steganography using RSA Algorithm and Modified OPAP (MOPAP). Data privacy is need in today world for secure information transmission and reception. So what is the way and how we develop the new concept to secure and hide any information (text, image, audio, and video etc.) using steganography. In proposed method I am hiding the data in a compressed video by using RSA Algorithm and Modified Optimal Pixel Adjustment Process (OPAP). The secret text data is first encrypted by using RSA algorithm. This encrypted message is transformed into bits and replaced it with the least significant bits (LSB) of discrete cosine transform (DCT) coefficients of digital frames in a video. We can provide elevated security to the embedded text data. This algorithm was tested on different types of videos format such as AVI, MPEG etc. The proposed method is expected to execute well and is compared to all existing method.**

Index Terms— **Cryptography ,Modified Optical Pixel Adjustment Process (MOPAP), RSA Algorithm, Steganography.**

I. INTRODUCTION

The word steganography is derived from the Greek words stego meaning cover and grafia meaning writing defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication .It is the practice of embedding secret information such that the existence of the information is not visible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding process to restrict detection or extraction of the embedded data.

Steganography
Steganography is a technique of information security that hides secret information (text, digital image, audio, video, etc) within a normal carrier media, such as digital image, audio, video, etc.

Cryptography: Cryptography is about protecting the content of messages.

Encrypt the message before sending to the destination no need of carrier/cover medium.

Manuscript received June 07, 2016
Ram Chandra Patnaik, Student, ME Communication, ETC Deptt., SSTC,SSGI,Bhilai
Himani Agrawal, Associate Professor, ETC Deptt., SSTC,SSGI,Bhilai

Breaking of cryptography is known as Cryptanalysis.

STEGO analysis
An attempt to detect and extract the hidden secret information from a carrier media is known as STEGO analysis.

This proposed method is based on An Efficient Video Steganography using RSA and Modified OPAP. In proposed method I am hiding the secret data in a compressed video by using modified optimal pixel adjustment process (MOPAP). Secrete Message is first encrypted by using cryptography algorithm. This encrypted message is transformed into bits and replaced with the least significant bits of discrete cosine transform coefficients of digital frames in a compressed video. The proposed method is expected to perform well and is compared to a Least Significant Bit replacement algorithm.

In proposed literature Discrete Cosine Transform (DCT) is using to enhance the security against steganalyst. The cover video is segmented into smaller matrix of size 8 x 8 (or 16 x 16) and transformed to DCT domain. The message bits are encrypted and embedded into DCT coefficients of selected cover frame. The proposed scheme encrypts the secret information before embedding it in the frame. The time complexity of the overall process will increase but at the same time the security achieved at this cost. This proposed method can withstand steganalysis process, because it is encrypted using RSA algorithm and Modified OPAP Algorithm. The performance results in terms of PSNR values are expected better in the proposed algorithm compared to the existing algorithm. The future work can be increasing the better quality of the video while maintaining high data and video rate, robustness and low distortions for different payloads in real time steganography.

$$\text{Quantized Value} = \frac{DCT\ (i,\ j)}{Quantization\ factor\ (I,\ j)}$$

A. Crisscross Ordering
We can use crisscross type scan pattern shown in fig.1 which rearrange the coefficient so that gathering the zero coefficient one often another, which is useful in lossless compression methods.

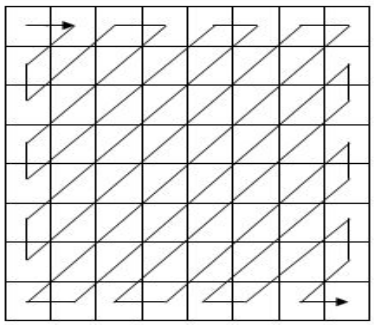

Fig. 4.1: Crisscross Ordering

B. RSA Algorithm

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman used for public key cryptography. It is also called as asymmetric key cryptography because two different keys are used for encryption and decryption process. It is based on PUBLIC and PRIVATE key.

The steps for key generation are:
Step 1: Generate two different primes p and q.
Step 2: Calculate the modulus n = p × q.
Step 3: Calculate the φ (n) = (p − 1) × (q − 1).
Step 4: Select for public exponent an integer e such that 1<e < φ (n) and gcd (φ (n), e) = 1.
Step 5: Calculate for the private exponent a value for d such that d = e−1 mod φ(n).
Step 6: Public Key = [e, n].
Step 7: Private Key = [d, n].

After obtaining cipher text, it is converted into bits and embedded in the selected frame by using modified optimal pixel adjustment method.

C. MOPAP Algorithm

In this section, Modified Optimal Pixel Adjustment Process (OPAP) is proposed to enhance the image quality of the stego-frame obtained by the simple DCT of least significant bit substitution method. MOPAP is a simple and efficient method to reduce the distortion caused by LSB replacement.

The MOPAP method is described as: let the pixel value is P, then

$$P'' = \begin{cases} P' + 2^b & P^{(b)} - q > 2^{(b-1)} \text{ and } P' + 2^b \le 255 \\ P' - 2^b & P^{(b)} - q > -2^{(b-1)} \text{ and } P' - 2^b \ge 0 \\ P' & \text{Otherwise} \end{cases}$$

Here P" denotes the result obtained by OPAP embedding.

D. Embedding Process

In embedding process, the cipher text bits obtained from RSA Algorithm are embedded by using Modified OPAP Algorithm.
The steps for embedding process are:
Step 1: For every component divide cover image into 8 X 8 pixel block.
Step 2: Apply 2D-DCT on each block obtain AC & DC Coefficients.
Step 3: Using specified quality factor quantize the coefficients.
Step 4: Skip the zero & DC coefficients.
Step 5: Convert text data into cipher text by using: $C = M^e \bmod n$, where [e, n] is encrypted key used at transmitter.
Step 6: Convert cipher text data into bits.
Step 7: Embed cipher text data bits into least significant bits of DCT coefficients by using OPAP algorithm.
Step 8: The stego frame obtained in the DCT domain is converted into the spatial domain using IDCT.

Block diagram of Embedding Steganography is shown below:

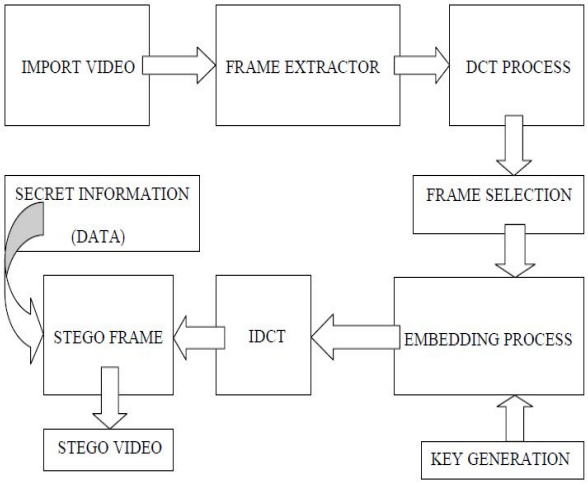

Fig. 4.2: Embedding Steganography Process

E. Extracting Process

In extracting process, we extract the cipher text bits from DCT coefficients and convert cipher text bits into message by using decryption key obtained from RSA algorithm.
The steps for Extracting Process are:
Step 1: The stego frame is segmented into 8*8 blocks.
Step 2: The 8*8 blocks are transformed into frequency domain using DCT.
Step 3: Extract cipher text data bits from each DCT coefficients.
Step 4: Convert the cipher text data bits into message bits by using decryption key [d, n].
Step 5: Convert message bits into text form.

Block diagram of Extracting Steganography is shown below:

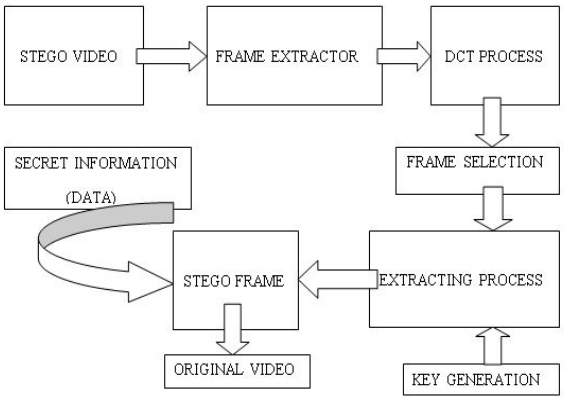

Fig. 3: Extracting Steganography Process

II LITERATURE REVIEW

S.NO	TITLE	AUTHOR	NAME OF JOURNAL	REMARKS	CONCLUSION DRAWN
1	Information hiding—A survey	F.A.P. Petitcolas, R.J. Anderson, and M. G. Kuhn	International Journal of electronics, Communication & Soft Computing Science & Engineering, IEEE 1999 Conference	Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks.	In this paper we gave an overview of information hiding in general and steganography in particular. We then described a number of attacks on information hiding systems.
2	Video watermark technique in motion vector	J. Zhang, J. Li, and L. Zhang	International Journal of IEEE 1530-1834/01, 2001 IEEE	In this paper, we propose a video watermarking technique to hide copyright information in MPEG motion vector.	To embed watermark information in motion vector has some good performances for hiding copyright information in the MPEG video sequence.
3	An Additive Approach to Transform-Domai n Information Hiding and Optimum Detection Structure	Qiang Cheng and Thomas S. Huang, Fellow, IEEE	IEEE Transaction on Multimedia, VOL. 3, NO.3, SEPTEMBER 2001	This paper presents an additive approach to transform-domain information hiding and the performance analysis for images and video.	The optimum detector structure is presented as opposed to the commonly used correlator. Our system provides both good transparency and precise control of detection errors. It can be applied to authentication, copyright protection, fingerprinting, and steganography.
4	The Use of Steganography to enhance error detection and correction in MPEG-2 Video	David L. Robie, Ning Wu and Russell M. Mersereau	International conference on Signal, system and computer IEEE Publication 0-7803-7576-9/02 /2002 IEEE	The transmission of data is always subject to corruption due to errors; however, video transmission, because of its real time nature must often deal with these errors. This MPEG-2 compliant codec uses data hiding principles to transmit parity checking information for the DCT coefficients.	This paper presents the Paritycodec, which uses steganography to encode error detection data. This hidden information comes at an imperceptable decrease in picture quality without impacting the total bit rate.
5	Dynamic Steganography Adds Additional Data Security	Richard Zavaleta, Subbarao Wunnav	IEEE Publication 0-7803-8367-2/04 / 2004 IEEE	This paper presents the concept of basic steganography and further improvements as well as the attacks on steganography.	Steganography add an extra layer of security to encrypted files by hiding them into other files. Multimedia files are ideal for embedding due to the large amount of data, especially video bmp files and audio wav files.

6	Steganography in Compressed Video Stream	Chengqian Zhang, Yuting Su, Chuntian Zhang	First International Conference on Innovative Computing, Information and Control (ICICIC'06) IEEE 2006	In this paper, a steganographic algorithm in MPEG compressed video stream was proposed. In each GOP, the control information for to facilitate data extraction was embedded in I frame, in P frames and B frames.	A steganographic algorithm for data embedding in video was proposed in this paper, operating directly in compressed bit stream. By embedding control information in I frame and redundant embedding in P and B frames, the capability of resisting video processing was achieved and a good balance between embedding capacity and security was obtained, but part of embedding capacity was sacrificed.
7	Data Hiding in H. 264 Encoded Video Sequences	Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras	IEEE 9th Workshop on Multimedia signal processing 2007, 1-4244-1274-9/07 /IEEE 2007	The proposed method takes advantage of the different block sizes used by the H.264 during the inter prediction stage in order to hide the desirable data. It is a blind data hiding scheme.	In this paper we present a new data hiding scheme for H.264. Its main advantage is that it is a blind scheme and its affect on video quality or coding efficiency is almost negligible.
8	A Secure Covert Communication Model Based On Video Steganography	Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb	IEEE Military Communication Conference MILCOM 2008, 978-1-4244-2677-5/08/ IEEE Publication 2008	This paper presents the model presented is based on pixel-wise manipulation of colored raw video files to embed the secret data.	This paper presents video-based steganographic model which utilizes cover video files in spatial domain to conceal the presence of other sensitive data regardless of its format. The proposed model is more secure against attacks because it depends on a list of security parameters.
9	Complete Video Quality Preserving Data Hiding with Reversible Functionality	KokSheik Wong, Kiyoshi Tanaka	3rd International Symposium on Communication, Control and Signal Processing (ISCCSP) 2008, 978-1-4244-1688-2/08/ 2008 IEEE Malta, 12-14 March 2008	This paper proposes a novel data hiding method in the MPEG domain where the image quality of the modified video is completely preserved to that of the original (compressed) video.	This method can reproduce the original video from the modified video, and hence reversible functionality is also achieved. The problem of filesize increase can be suppressed with any of the three independent solutions by trading off with payload and coding efficiency.
10	A New Video Steganalysis Algorithm against Motion Vector Steganography	Chengqian Zhang, Yuting Su, Chuntian Zhang	National High Technology Research and Development Program of China (No.2006AA01Z407) 978-1-4244-2108-4/08/2008	In this technique is proposed against the video stegnanography methods which hide the secret message by least modification of the motion vectors.	According to this paper it deals with data hiding in compressed video.
11	A Novel Steganographic Algorithm Based on the Motion	Xuansen He, Zhun Luo	International Conference on Computer Science and Software	Most data hiding techniques in digital video utilize I frame to embed the secret	The experimental results show that our algorithm not only can embed large amounts of the secret information into a video

	Vector Phase		Engineering, 2008, DOI 10.1109/CSSE.2008.359	information so the capacity of P and B frame is wasted. In order to improve the embedding efficiency we use the matrix encoding.	but also can maintain good video quality. Once only one motion vector is modified at most so that the Motion Vector modification rate is decreased.
12	Error-Resilient Transmission for 3D-DCT Coded Video	Donald A. Adjeroh, Member, IEEE, and Supriya D. Sawant	IEEE Transaction on Broadcasting, VOL. 55, NO. 2, JUNE 2009	Two key challenges are compression and effective error protection against channel errors. Based on the statistical and structural properties of 3D DCTcoefficientswe propose different data partitioning schemes for their unequal error protection.	We have studied the problem of unequal error protection for transmitting video at very low bit rates, when the compression method is based on the three-dimensional discrete cosine transform. Based on the grouping, we described techniques for allocation of the available redundancy among the different groups. In video data transmission often it comes in bursts, and hence could affect more than one block of data.
13	Improving the Perturbed Quantization Steganography by Modified Matrix Encoding	Xuexiu Zhu, Weiming Zhang, Jianqing Qi, Jiufen Liu	IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS) 978-1-4244-5849-3/10/ 2010 IEEE	Perturbed Quantization and Modified Matrix Encoding are two efficient embedding methods for JPEG steganography, in which the sender uses the side information of quantizing procedure of DCT coefficient.	By fusing modified matrix encoding (MME) and wet paper codes, the proposed method can reach low average distortion and avoid modification in some sensitive areas of the cover, and therefore improve the security of the steganography.
14	Chaos based Spatial Domain Steganography using MSB	Sathisha1 N, Madhusudan G N, Bharathesh S, Suresh Babu K, Raja K B, Venugopal K R	5th International Conference on Industrial and Information Systems, ICIIS, 978-1-4244-6653-5/10/2010 IEEE 2010, Jul 29 - Aug 01, 2010, India	In this paper we propose Spatial Domain Steganography using 1-Bit Most Significant Bit (MSB) with chaotic manner. The first block of cover image is embedded with 8 bits of upper bound and lower bound values required for retrieving payload at the destination.	The proposed algorithm has better capacity and security with high PSNR compared to existing algorithm. In future the same technique can be extended to the transform domain and robustness of algorithm can be verified.
15	Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error	Hussein A. Aly, Member, IEEE	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1,	This paper deals with data hiding in compressed video. We target the motion vectors used to encode and reconstruct both the forward predictive	According to this paper it deals with data hiding in compressed video. We proposed a new data-hiding method in the motion vectors of MPEG-2 compressed video. Unlike most data-hiding methods in the motion vectors that rely their selection on

			MARCH 2011	(P)-frame and bidirectional (B)-frames in compressed video.	attributes of the motion vectors macroblocks prediction error is high (low PSNR).
16	A Novel Steganography Method for Image Based on Huffman Encoding	Rig Das, ThemrichTuithung	3rd National Conference on Emerging Trend and Applications in Computer Science (NCETACS) IEEE Publication 978-1-4577-0748-3/12/ 2012	This paper presents a Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the LSB of each of the pixel's intensities of cover image.	The algorithm improves the security and the quality of the stego-image and is better in comparison with other existing algorithms. The proposed method may be more robust against brute force attack.
17	Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering	Tamer Shanableh	IEEE Transaction on Information Forensic and Security, Vol. 7, No. 2, April 2012	This paper proposes two data hiding approaches- the first approach hides message bits by modulating the quantization scale of a constant bitrate video. A second order multivariate regression is used. The regression model is then used by the decoder to predict the values of the hidden message bits with very high prediction accuracy. The second approach uses the flexible macroblock ordering feature of H.264/AVC to hide message bits.	In the first approach, the quantization scale of a CBR video is either incremented or decremented according to the underlying message bit. A second-order multivariate regression is used to associate macroblock-level features with the hidden message bit. The decoder makes use of this regression model to predict the message bits.
18	An Efficient Method for Steganography in Videos	N. Sarath Babu, Dr. M. Sailaja	International Journal of Research in Computer and Communication Technology, Vol 2, Issue 8, August - 2013	This paper applies steganography algorithm in videos. In proposed method we are hiding the data in a compressed video by using OPAP.	The proposed scheme used in this paper encrypts the secret information before embedding it in the frame. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it.

CONCLUSION

The steganography is used in the covert communication to transport secrete information. The cover video will be segmented into smaller matrix of size 8x8 and converted to DCT domain. The message bits will be encrypted and embedded into DCT coefficients of selected cover frame. It is highly secured because the steganalysis methods will result in

random and inappropriate data which is difficult to arrange in proper and correct format.

ACKNOWLEDGMENT

I THANKFUL TO MRS .HIMANI AGRAWAL FOR HERSUPPORTING IN THIS PEOJECT

REFERENCES

[1] Petitcolas F.A.P., Anderson R.J., and Kuhn M.G., 1999, —"Information hiding—A survey", Proc. IEEE, vol. 87, no. 7, pp. 1062-1078.

[2] Zhang J., Li J., and Zhang L., 2001 —"Video watermark technique in motion vector", in Proc. XIV Symp. Computer Graphics and Image Processing, pp. 179-182.

[3] Qiang Ch. and Thomas S. Hu., 2001 —"An Additive Approach to Transform-Domain Information Hiding and Optimum Detection Structure", Proc. IEEE, vol. 3, no. 3, pp. 273-284.

[4] Robie D. L., Ning Wu and Russell M. Me., 2002—" The Use of Steganography to Enhance Error Detection and Correction in MPEG-2 Video", Proc. IEEE, vol. 2, pp. 1204-1209.

[5] Zavaleta,R., Subbarao W.,2004—" Dynamic Steganography Adds Additional Data Security", Proc. IEEE, vol. 4, pp. 550-563.

[6] Xu C., Ping X., and Zhang T., 2006, —"Steganography in compressed video stream", in Proc. Int. Conf. Innovative Computing, Information and Control (ICICIC'06), vol. II, pp. 803-806.

[7] Kapotas S. K., Varsaki E. E., and Skodras A. N., 2007, —"Data hiding in H.264 encoded video sequences", in IEEE 9th Workshop on Multimedia Signal Processing (MMSP07), pp. 373-376.

[8] He X. and Luo Z., 2008, —"A novel steganographic algorithm based on the motion vector phase", in Proc. Int. Conf. Comp. Sc. and Software Eng., pp. 822-825.

[9] Chengqian Z., Yuting Su, Chuntian Z., 2008, "A New Video Steganalysis Algorithm against Motion Vector Steganography," Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on, vol. 08, pp.1-4.

[10] Amr A. H., Gouda I. S. and Yahya Z. M., 2008, —" A Secure Covert Communication Model Based On Video Steganography", IEEE Military Communication Conference MILCOM, Vol. no.-8, pp. 1-6, 16-19.

[11] KokSheik W., Kiyoshi T., 2008, —" Complete Video Quality Preserving Data Hiding with Reversible Functionality", 3rd International Symposium on Communication, Control and Signal Processing (ISCCSP), Vol. no.-8, pp. 1029-1034.

[12] Donald A. Adjeroh, Member, IEEE, and Supriya D. Sawant, 2009, —" Error-Resilient Transmission for 3D-DCT Coded Video", IEEE Transactions on Broadcasting, Vol. no.-55, pp. 178-189.

[13] Xuexiu Z., Weiming Z., Jianqing Qi, Jiufen L., 2010, , —" Improving the Perturbed Quantization Steganography by Modified Matrix Encoding", IEEE International Conference on Wireless Communications, Networking and Information Security(WCNIS), Vol. no.-10, pp. 437-440.

[14] Sathisha1 N, Madhusudan G N, Bharathesh S, Suresh Babu K, Raja K B, Venugopal K R, 2010, —" Chaos based Spatial Domain Steganography using MSB", 5th International Conference on Industrial and Information Systems, ICIIS, Vol. no.-10, pp. 177-182.

[15] Hussein A., 2011—"Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error" IEEE Trans on Information Forensics and Security, Vol. 6, No. 1, pp. 14-17.

[16] Rig D., ThemrichT., 2012 —" A Novel Steganography Method for Image Based on Huffman Encoding" IEEE 3rd National Conference on Emerging Trend and Applications in Computer Science (NCETACS), Vol. 6, No. 1, pp. 14-17.

[17] Tamer S., 2012. —"Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering" IEEE Transaction on Information Forensic and Security, Vol. 7, No. 2, pp. 455-464.

[18] Sarath Babu N., Dr. Sailaja M., 2013 —" An Efficient Method for Steganography in Videos" International Journal of Research in Computer and Communication Technology, Vol. 2, No. 8, pp. 644-648.