PERFORM VIDEO BASED DATA HIDING AND ENCRYPTION

[1] Ms.N.Nanthini,

M.Sc., M.Phil Assistant Professor,

[2] M. Nirmala,

M.Sc (Computer Science),

[1] [2] Department Of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram.

ABSTRACT

Video data hiding is a very important research topic. Security of information is major concern of information technology and communication. This project introduces elliptical curve cryptography and Least Significant bit substitution technique for hiding data in video file. The Steganography is a way to hide secret information behind an innocent cover file. This project uses the concept of video Steganography, where the data is hidden behind the frames of videos. In this project data hiding a form of cryptography embeds data into digital media for the purpose of identification, annotation. These algorithms are a basic algorithm of encryption and decryption for data hiding. The framework is tested by all kind of videos such as .mp4, .3gp, .avi etc., and gets successful output for all video data hiding process. The proposed scheme is based on key stream generator for confusion process. The confusion process is initiated by a secret key of 256 bits which is itself generated by a logistic map. To make the cipher more dynamic against any attack, the secret key is modified after encrypting each block of the image. The experimental results show that the proposed method provides an efficient and secure way for real-time image encryption and transmission. The proposed scheme used by security, while hiding the video to provide security for encrypts and decrypt process. The simulation results show that the process of hiding the video by security.

Index Terms - Video Data hiding, Encryption, Decryption, Decryption, Security, and RSA.

I INTRODUCTION

1.1 INTRODUCTION TO IMAGE PROCESSING

In imaging science, image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it.

Image processing usually refers to digital image processing, but optical and analog image processing also are possible. This article is about general techniques that apply to all of them. The acquisition of images (producing the input image in the first place) is referred to as imaging.

Closely related to image processing are computer graphics and computer vision. In computer graphics, images are manually made from physical models of objects, environments, and lighting, instead of being acquired (via imaging devices such as cameras) from natural scenes, as in most animated movies. Computer vision, on the other hand, is often considered high-level image processing out of which a machine/computer/software intends to decipher the physical contents of an image or a sequence of images (e.g., videos or 3D full-body magnetic resonance scans).

In modern sciences and technologies, images also gain much broader scopes due to the ever growing importance of scientific visualization (of often large-scale complex scientific/experimental data). Examples include microarray data in genetic research, or real-time multi-asset portfolio trading in finance.

1.2 DATA HIDING

In first I have addressed a few fundamental issues of data hiding in image and video. We have proposed general solutions, including how to embed multiple bits, how to handle uneven embedding capacity, and how to allow the number of reliably extractable bits to be adaptable to the actual noise condition. Here apply the solutions to specific design problems and present details of embedding data in image and video.

In Section II, we embed data in images at two levels, each of which is designed for different robustness. This approach al-lows for graceful decaying of extractable information as noise gets stronger. In extend the multilevel embed-ding to video, for which difficulty arises because the embedding capacity varies from region to region within a frame as well afro frame to frame. We embed control information to facilitate the extraction of the user data payload and to combat such distortions as frame jitter.

1.3 VARIOUS DATA HIDING METHOD

Data Hiding Techniques in Still Images Nosrati et al. introduced a method that embeds the secret message in RGB 24 bit color image. This is achieved by applying the concept of the linked list data structures to link the secret messages in the images.

First, the secret message that is to be transmitted is embedded in the LSB‟s of 24 bit RGB color space. Next, like the linked list where each node is placed randomly in the memory and every node points to every other node in list, the secret message bytes are embedded in the color image erratically and randomly and every message contains a link or a pointer to the address of the next message in the list.

Also, a few bytes of the address of the first secret message are used as the stego - key to authenticate the message. Using this technique makes the retrieval and the detection of the secret message in the image difficult for the attacker. Kuo et al. presented a reversible technique that is based on the block division to conceal the data in the image.

1.4 VARIOUS DATA HIDING TECHNIQUES

All presented techniques to hide data in the still images and generated stego - images as the output. In embed the data in RGB 24 bit color image by using the linked data structures where in, the data hidden in the image is linked with other data.

The advantage of this method is that hiding the data randomly than sequential will make it difficult for the attacker to locate it and also without the authentication key the attacker will not be able to access the next piece of data in the image.

1.5 CRYPTOGRAPHY

The art of protecting the information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

1.6 THE PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription.

Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans.

It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

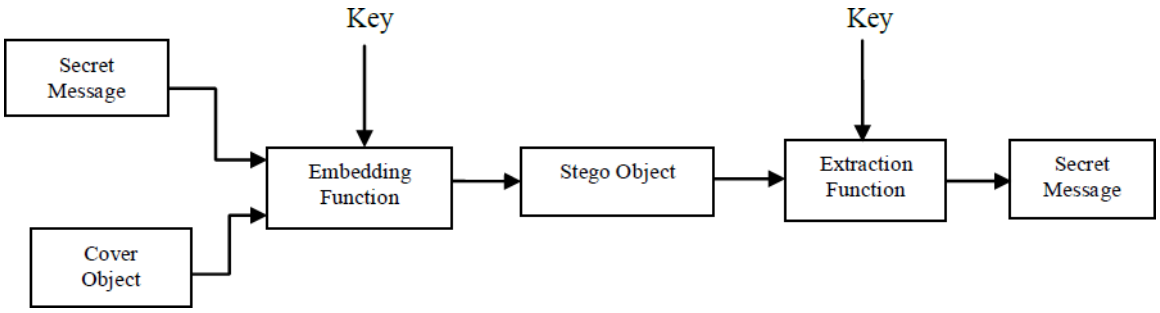


Figure 1.1 a model of the steganography process with cryptography

II LITERATURE SURVAY

S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, "Data hiding inH.264 encoded video sequences," in IEEE 9th Workshop on Multimedia Signal Processing (MMSP07), Oct. 2007, pp. 373–376.

The widespread of the Internet and World Wide Web has changed the way digital data is handled. The easy access of images, musical documents and movies has modified the development of data hiding, by placing emphasis on copyright protection, content-based authentication, tamper proofing, annotation and covert communication.

Data hiding deals with the ability of embedding data into a digital cover with a minimum amount of perceivable degradation, i.e., the embedded data is invisible or inaudible to a human observer. Data hiding consists of two sets of data, namely the cover medium and the embedding data, which is called the message.

The digital medium or the message can be text, audio, picture or video depending on the size of the message and the capacity of the cover. Early video data hiding approaches were proposing

still image watermarking techniques extended to video by hiding the message in each frame independently.

Methods such as spread spectrum are used where the basic idea is to distribute the message over a wide range of frequencies of the host data. Transform domain is generally preferred for hiding data since, for the same robustness as for the spatial domain; the result is more pleasant to the Human Visual System (HVS). For this purpose the DFT (Discrete Fourier Transform), the DCT (Discrete Cosine Transform), and the DWT (Discrete Wavelet Transform) domains are usually recent video data hiding techniques are focused on the characteristics generated by video compressing standards.

Motion vector based schemes have been proposed for MPEG algorithms. Motion vectors are calculated by the video encoder in order to remove the temporal redundancies between frames.

In these methods the original motion vector is replaced by another locally optimal motion vector to embed data. Only few data hiding algorithms considering the properties of H.264 standard have recently appeared in the open literature. In subset of the 4×4 DCT coefficients are modified in order to achieve a robust watermarking algorithm for H.264.

In [9] the blind algorithm for copyright protection is based on the intra prediction mode of the H.264 video coding standard. In some skipped macro blocks are used to embed data.

The well established H.264/AVC video coding standard has various motion compensation units in sizes of 16×16, 16 ×8, 8×16, 8×8, and sub8×8 [11]. For sub8×8, there are further four sub-partitions of sub8×8, sub8×4, sub4×8, and sub4 ×4. In this paper we propose a new data hiding scheme, which takes advantage of the different block sizes used by the H.264 encoder during the inter prediction, in order to hide the desirable data. The message can be extracted directly from the encoded stream without knowing the original host video.

This method is best suited for content-based authentication and covert communication applications. Embedding takes place during the encoding process and utilizes the advanced inter prediction features of the H.264 encoder. Its main advantage is that it is a blind scheme and its affect on video quality or coding efficiency is almost negligible.

It is highly configurable, thus it may result in high data capacities. Finally, it can be easily extended, resulting in better robustness, better data security and higher embedding capacity.

ADVANTAGES

- Does not actually affect the PSNR of the inter frames.
- To perform the best possible inter prediction during its normal operation.

DISADVANTAGES

- The frame period is too small and the algorithm repeats the message very often.

III THEORETICAL BACKGROUND

3.1 PROBLEM IDENTIFICATION

There are many researches that have been proposed for hiding the data into digital videos. Most of those schemes uses the attributes of motion vectors like amplitude, phase angle etc. This project deals with hiding data in compressed video where motion vectors are used to encode and reconstruct both the forward predictive (P-) frame and bidirectional (B-) frames in the compressed video.

The subsets of motion vectors are chosen based their associated macro block prediction error. Pertinent features will be collected from the motion in between the frames as in the form of the vectors in association with macro blocks and depending on the motion message is going to be hidden.

To achieve the robustness an adaptive threshold is searched and low predictive error level is retained. Secret message bits are hidden in least significant bit of both components of candidate motion vector. The valuation will be based on two criteria: minimum distortion to reconstructed video and minimum overhead on compressed video size.

DISADVANTAGES

- However, they may not provide accurate results for sequences with no or small object motions.
- The disparity estimation is another challenging task, requiring heavy computational loads.
- The interactions prevent them from being used in applications in which full automation is required.

3.2 PROBLEM SOLVING

This project aims to explain the data hiding concept in motion vector of compressed video. In this data hiding in motion vector is done by stenography Technique, data is compressed in different frames of video. The process starts with Mailing system such as sending and receiving secret data.

In that hiding data in natural sequence of multiple groups of pictures. The RSA algorithm is used for encryption of message in video and use edge detection mechanism for selecting pixel, Data is encoded as a region where motion estimation is allowed to generate motion vector. The sender first uses the stenographic application for encrypting the secret message.

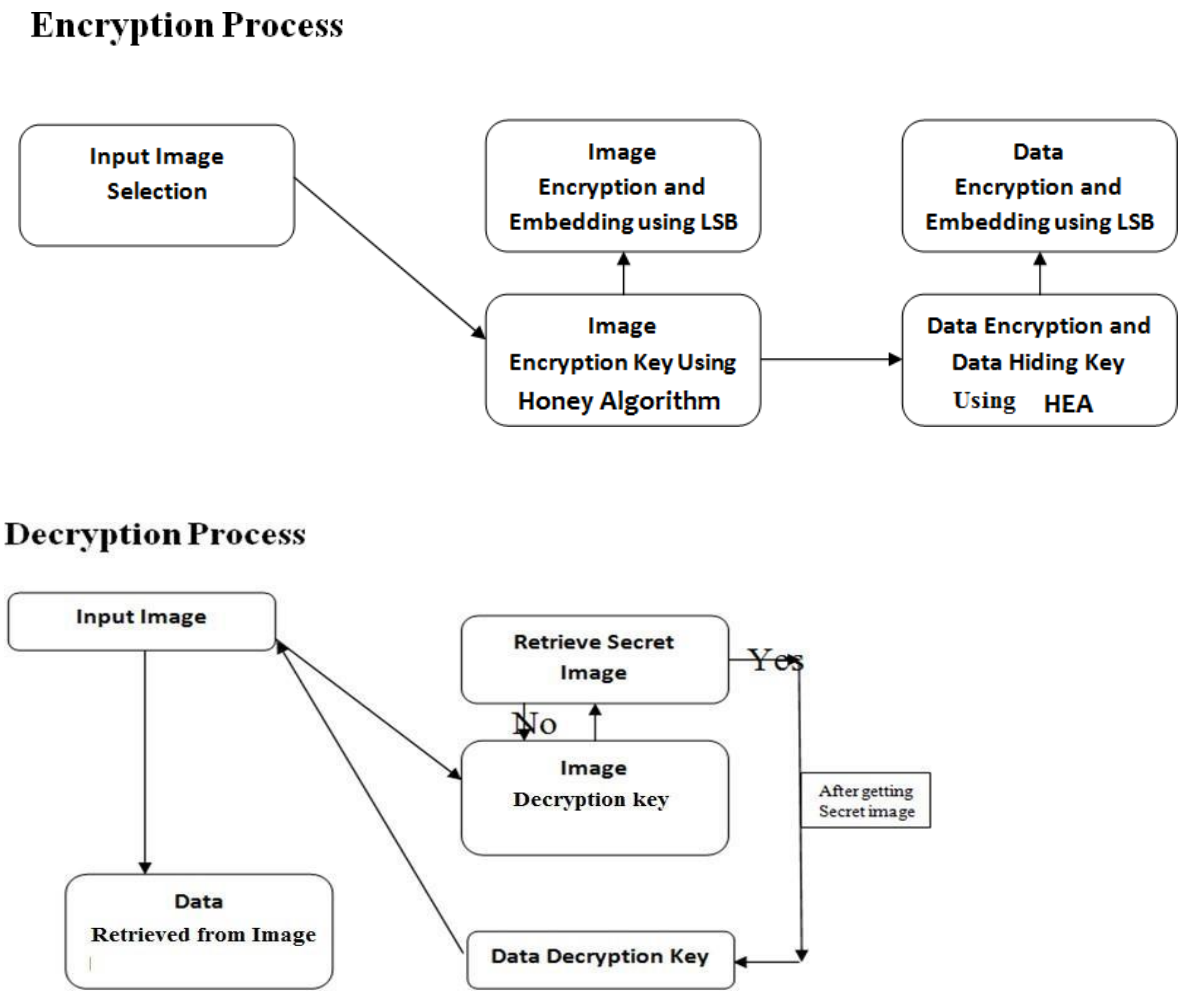
For this encryption, the sender uses text document in which the data is written and the image as a carrier file in which the secret message or text document to be hidden. The sender sends the carrier image and text document to the encryption phase for data embedding, in which the text document is embedded into the image file. In encryption phase, the data is embedded into carrier file which was protected.

The decryption phase decrypts the original text document using the least significant bit decoding and decrypts the original message. The performance analysis shows that the algorithm ensures better security against attackers.

ADVANTAGES

- Improve the classification accuracy because the extraction of features can be restricted to the subset of pixels contained in the OOI of the images.
- Automatic segmentation of OOIs in low DOF images to improve search quality.

3.3 SYSTEM ARCHITECTURE



IV SYSTEM IMPLEMETATION

4.1. INPUT VIDEO

First to process the input video using pre processing technique for reduce noise of video. No of frames is converted form video then will proceed on image. Preprocessing is the key step and the starting point for image analysis, due to the wide diversity of resolution, image format, sampling models, and illumination techniques that are used during acquisition. In our framework, preprocessed images are then subject to analysis under different models, which are going to be evaluated in parallel in a multi agent system for identifying the security.

4.2. ENCRYPTION OF IMAGE & SECRET DATA

In our proposed system, first of all we select a true color image of size 512 x 512 for to it as a cover image and a secret message which will be embedded in the cover image. Image encryption can be used to watermark digital images for copyright purposes and to make your personal images safe from prying eyes. For images that are stored on laptops, smart phones, or in the cloud, encryption gives you an extra layer of security to help keep your images private.

Steganography is a way of hiding messages within an image, text, or even in video, but it is not a true encryption process. With digital images, a second picture may be hidden inside a first by selectively replacing some of the binary data that represent each pixel's color and intensity with opposite values.

One common steganography method, called the least significant bit method, changes the unit values of the binary image data so ones become zeros and zeros become ones. Only a portion of the binary image data needs to be changed to hide another picture. Steganography may be used to add digital watermarks to images to help protect copyrighted material from theft, but it can also be used to hide stolen data or sensitive information.

4.3. TRANSMISSION

In that module the encrypted or cover image will be transmit to the receiver side.RSA encryption/decryption the test image Cameraman sized 256 *256 was used as the original cover in the experiment. Then, we embedded data into the encrypted image by using LSB method. The encrypted image with message is the encrypted file by public key. The extracted information that was decrypted by the private key.

4.4. DECRYPTION PROCESS

Reverse the process of encryption work. This is major work for retrieval process. Once the process completed then will retrieve the original input and secret message or else cat get the original video and secret message.

4.5 PERFORMANCE COMPARISON

I am performed several experiments to evaluate the performance of the proposed coding scheme for data hiding and encryption, decryption methods. I am analyzed the former under encryption and decryption of images, extract the data. Also, we tested the proposed code for expression recognition with RSA algorithm.

The objective of the work have been implemented an image steganography technique using encryption and decryption method with RSA algorithm to improve the security of the data hiding technique. This technique is a combination of one steganography technique and one cryptographic technique which enhances the security of data and data hiding technique.

Our implemented encryption and decryption method technique on images is used to hide information in the RGB pixels value of the cover image in the form of 3, 3, and 2 bit order and positions to hide the data bits have been calculated by hash function. The use of RSA algorithm has made our technique more secure for open channel.

RSA algorithm has been used with encryption and decryption method so that the original text will be embedded into cover image in the form of cipher text. The decryption method technique has been applied to true color images and which gives satisfactory results. The performance of the encryption and decryption method technique has been evaluated and graphically represented on the basis of two measures are – Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) and obtained values are much better than existing techniques. The technique called “A Secure Steganography Based on RSA Algorithm and encryption and decryption method Technique” has been implemented on MATLAB tool by analyzing four color images of size 512 x 512 tiff format as selected to hide a fixed size of secret data. In this process stego-image is generated using decryption method and RSA encryption which carried out to enhance the security of hidden data.

V CONCLUSION & FUTURE WORK

5.1 CONCLUSION

In this project I am providing high security for data by using Data Hiding in Motion Vector of Compressed video. The two types of security provided are through by using steganography as well as E-mail system. By compression large amount of data are transmitted.

The above techniques providing protection for data from hackers. So this is different technique as compared to older methods. In these techniques robustness is increased and there is no loss of data, and more reliable system.

5.2 FUTURE ENHANCEMENT

In the future, I will propose digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. For the purpose of content notation and/or tampering detection, it is necessary to perform data hiding in these encrypted videos. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content.

In addition, it is more efficient without decryption followed by data hiding and re-encryption. In this project, a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed, which includes the following three parts, i.e., H.264/AVC video encryption, data embedding, and data extraction.

By analyzing the property of H.264/AVC codec, the code words of intraprediction modes, the code words of motion vector differences, and the code words of residual coefficients are encrypted with stream ciphers.

Then, a data hider may embed additional data in the encrypted domain by using codeword substitution technique, without knowing the original video content. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. Furthermore, video file size is strictly preserved even after encryption and data embedding. Experimental results have demonstrated the feasibility and efficiency of the proposed scheme.

REFERENCE

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

[2] C. Xu, X. Ping, and T. Zhang, “Steganography in compressed video stream,” in Proc. Int. Conf. Innovative Computing, Information and Control (ICICIC’06), 2006, vol. II, pp. 803–806.

[3] Hussein A. Aly ―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, Mar 2011.

[4] X. He and Z. Luo, ―A novel Steganography algorithm based on the motion vector phase,‖ in Proc. Int. Conf. Comp. Sc. and Software Eng., 2008, pp. 822– 825

[5] K B Shiva Kumar, K B Raja, R K Chhotaray, SabyasachiPattanaik. "Bit length replacement steganography based on dct coefficients."International Journal of Engineering Science and Technology (2010): 3561-3570.

[6] R. Chandramouli, N. Memon, "Analysis of LSB based image Steganography techniques", International Conference on Image Processing, Vol. 3, Pages No. 1019 – 1022, 07 Oct 2001-10 Oct, 2001.

[7] WeiqiLuo, Fangjun Huang, Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 – 214, June, 2010.

[8] Ross J. Anderson, Fabien A. P. Petit colas, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481, May, 1998.

[9] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong-Yee Lee, "A High Capacity 3D Steganography Algorithm", IEEE Transactions on Visualization and Computer Graphics, Vol. 15, Issue No. 2, Pages No. 274 – 284, March April, 2009.

[10] Nicholas Hopper, Luis von Ahn, John Langford, "Provably Secure Steganography", IEEE Transactions on Computers, Vol. 58, Issue No. 5, Pages No. 662 – 676, May, 2009.

[11] Mohammad TanvirParvez, Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", Asia-Pacific Services Computing Conference, IEEE, Pages No. 1322 – 1327, 9-12 Dec., 2008.

[12] Jing-Ming Guo, Thanh-Nam Le, "Secret Communication Using JPEG Double Compression", Signal Processing Letters, IEEE, Vol. 17, Issue No. 10, Pages No. 879 – 882, Oct., 2010.

[13] WeiqiLuo, Yuangen Wang, Jiwu Huang, "Security Analysis on Spatial 1 Steganography for JPEG Decompressed Images", Signal Processing Letters, IEEE, Vol. 18, Issue No. 1, Pages No. 39 – 42, Jan., 2011.

[14] Dr.EktaWalia, PayalJainb, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Vol. 10, Issue No. 1, April, 2010.

[15] Mohammad A. Ahmad, Dr. ImadAlshaikhli, Sondos O. Alhussainan, "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No. 127-139, Sept., 2012.

[16] DeepeshRawat, VijayaBhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, Vol. 64, Issue No. 20, Feb., 2013.

[17] AnkitChaudhary, J. Vasavada, J. L. Raheja, S. Kumar, M. Sharma, "A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images", 22nd International Conference on Computer Graphics and Vision, 2012.

[18] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu, “A Comparative Analysis of Image Steganography”, International Journal of Computer Applications, Vol. 2, Issue No. 3, May, 2010.

[19] Samir Kumar Bandyopadhyay, SarthakParui, “A Method for Public Key Method of Steganography”, International Journal of Computer Applications, Vol. 6, Issue No. 3, Sept., 2010.

[20] P. Nithyanandam, T. Ravichandran, N. M.Santron, E. Priyadarshini, “A Spatial Domain Image Steganography Technique Based on Matrix Embedding and Huffman Encoding”, International Journal of Computer Science and Security (IJCSS), Vol. 5, Issue No. 5, 2011.

[21] Shailender Gupta, AnkurGoyal, Bharat Bhushan, “Information Hiding Using Least Significant Bit Steganography and Cryptography”, I. J. Modern Education and Computer Science, Vol. 6, Pages No. 27-34, 2012.

[22] MrithaRamalingam, “Stego Machine –Video Steganography using Modified LSB Algorithm”, World Academy of Science, Engineering and Technology, Pages No. 50, 2011.

[23] Deepali, “Steganography with Data Integrity”, International Journal of Computational Engineering Research, Vol. 2, Issue No. 7, 2012.

[24] Asad.M., Gilani, J., Khalid.A. “An enhanced least significant bit modification technique for audio steganography”, Computer Networks and Information Technology (ICCNIT), IEEE, Pages No. 143 – 147, 11-13 July, 2011.

[25] Information about cryptography, available at http://en.wikipedia.org/wiki/Cryptography.

[26] Chandra.M.Kota, CherifAissi, “Implementation of the RSA algorithm and its cryptanalysis”, ASEE Gulf-Southwest Annual Conference, American Society for Engineering Education, USA, 2002.

[27] Cancellable biometrics”, Information Processing Letters, vol. 93, no. 1, pp. 1-5, 2005.

[28] C.-S. Laih, and K. Y. Chen, "Generating visible RSA public keys for PKI", International Journal of Information Security, Vol. 2, No. 2, Springer-Verlag, Berlin, 2004, pp. 103- 109.

[29] X.Y. Jing and D. Zhang, “A face and palm print recognition approach based on discriminant DCT feature extraction”, IEEE Transactions, vol. 34, no. 6, pp. 2405-2415, 2004.

[30] X. Wu, D. Zhang, K. Wang, “Palm print classification using principal lines”, Pattern Recognition, vol. 37, no. 10, pp. 1987-1998, 2004.

[31] C. Poon, and H.C. Shen, “Personal identification and verification: fusion of palmprint representations”, Proceedings of International Conference on Biometric Authentication, pp. 782-788, 2004.

[32] F. Li, M.K.H. Leung and X. Yu, “Palm print identification using Hausdorff distance”, in Proceedings of International Workshop on Biomedical Circuits and Systems, pp. S3/3-S5-8, 2004.

[33] A. Okatan, C. Akpolat and G. Albayrak, “Palm print verification by using cosine vector”, IJSIT Lecture Note of International Conference on Intelligent Knowledge Systems, vol. 1, no. 1, pp. 111-113, 2004.

[34] S. Ribaric and N. Pavesic, “Multimodal biometric user-identification system for network-based applications”, IEEE Proceedings, 2003, 1-6.

[35] MS, "Public Key Cryptography-Applications Algorithms and Mathematical Explanations", Tata Elxsi Ltd, 2007