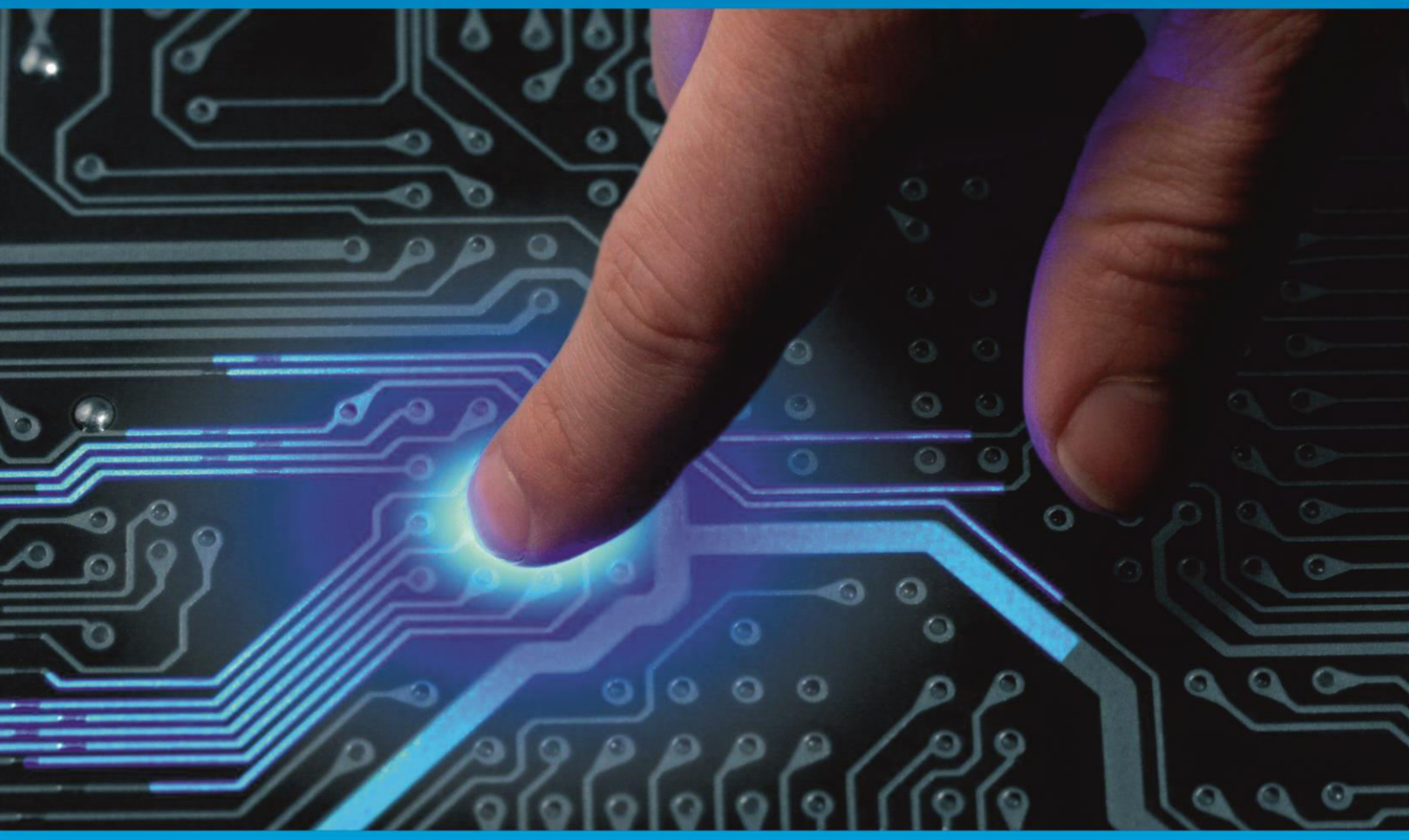
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903030 |

Comments on Steganograpy using Reversible Texture Synthesis

N. Kiruthika, R.Madhumathi.,MCA.,M.Phil

Student, Dept. of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, TamilNadu

Assistant Professor, Dept. of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, TamilNadu, India

ABSTRACT: Internet is gaining more and more popular now a days, so there is need to provide security for everything on internet. One of the most important concepts where we need to provide higher security is in communication between sender and receiver. Due to security threats the requirement of the secure transmission of the data is also increased the reason for developing the Data Hiding is the easy access of images, documents confidential data by the hackers who always monitor the system. Data hiding is the process of secretly embedding information inside a source without changing its content and meaning there is numerous techniques which hides the data. This paper aims to implement data hiding in compressed video. Like data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis. 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 file 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 with the password now the carrier file acts as an input for the decryption phase. The image in which data is hidden i.e. the carrier file is sent to the receiver using a transmission medium. E.g. Web or e-mail. The receiver receives the carrier file and places the image in the decryption phase. Now the carrier file acts as an input for the decryption phase. The image in which data is hidden the carrier image is sent to the receiver using a transmission medium. E.g. Web or e-mail. The receiver receives the carrier file and places the image in the decryption phase.

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 we 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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903030 |

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. The designs presented in this paper can be used as building blocks for such applications as copy control, access con-Manuscript received February 4, 2002; revised November 22, 2002. This work was supported in part by Panasonic Information and Networking Laboratory, by a R&D Excellence Grant from the State of New Jersey, and by the National Science Foundation CAREER Award CCR-0133704. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Bruno Carpentieri.M. Wu is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: minwu@eng.umd.edu).H. Yu is with Panasonic Information and Networking Laboratories (PINTL),Princeton, NJ 08540 USA (e-mail: heathery@research.panasonic.edu).B. Liu is with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: liu@ee.princeton.edu).Digital Object Identifier 10.1109/TIP.2003.810589trol, robust annotation, and content-based authentication. Comprehensive protection from malicious attacks that make watermarks undetectable would require both technical and business approaches, such as a well-determined business and pricing model. Our design objective here focuses on surviving common processing in transcoding and scalable/progressive transmission, such as compression with different ratio and frame rate conversion for video.

II. LITERATURE SURVEY

Data hiding in H.264 encoded video sequences

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 t o 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 t o 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 1 6 × 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903030 |

III. SYSTEM DESCRIPTION

3.1 EXISTING SYSTEM

There are many researches that have been proposed for hiding the data into digital videos. Most of those schemes uses t he attributes of motion vectors like amplitude, phase angle etc. This paper 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 a 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 evaluation will be based on two criteria: minimum distortion to reconstructed video and minimum overhead on compressed video size.

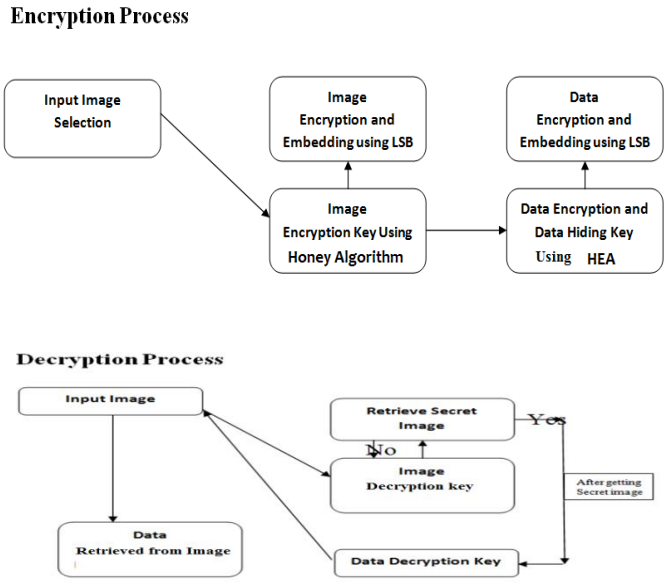
3.2 PROPOSED SYSTEM

This paper 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 ARCHITECTURE:



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903030 |

IV. SYSTEM IMPLEMENTATION

4.1 Input image

First to process the input image using pre processing technique for reduce noise of 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 multiagent system for identifying the security.

4.2 Encryption of image

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. Special software is needed to encrypt images and is readily available as freeware, shareware, and for sale on the Internet for all major operating systems.

Images are encrypted for many reasons, including identifying the creator of an image, protecting copyright information, deterring piracy, and blocking images from being viewed by users who shouldn't have access to them. By encrypting images, you can send them through email or over the Internet without worrying about your images are being viewed by people that you don't want to see them. Encrypting images on your home computer will also give you a measure of security in case a hacker gains access to your hard drive, and encrypting the images on your laptop or Smartphone will likewise make your images safer if your computer or laptop are lost or stolen.

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 steganographic 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. The test demonstrate that it is impossible to get the original information when input the wrong key which provides the protection to the hidden information.

4.4 Performance Comparison

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

V. EXPERIMENTAL RESULTS AND DISCUSSION

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 steganographic 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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903030 |

process stego-image is generated using decryption method and RSA encryption which carried out to enhance the security of hidden data.

VI. CONCLUSION AND FUTURE WORK

CONCLUSION

In this paper we are 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 technique is providing protection for data from hackers. So this is different technique as compared to older methods. By using above technique the robustness is increased and there is no loss of data, and more reliable system

VII. FUTURE WORK

In the future, we 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 paper, 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.

REFERENCES

[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 Steganographic algorithm based on the motion vector phase,‖ in Proc. Int. Conf. Comp. Sc. and SoftwareEng., 2008, pp. 822–825
[5] K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattanaik. "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] Weiqi Luo, 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. Petitcolas, “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 Tanvir Parvez, 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903030 |

[13] Weiqi Luo, 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.Ekta Walia, Payal Jainb, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Vol. 10, Issue No. 1, April, 2010.
[15] [17] Mohammad A. Ahmad, Dr. Imad Alshaikhli, 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] Deepesh Rawat, Vijaya Bhandari, "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] Ankit Chaudhary, 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. Deepika chowdavarapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications, Vol. 2, Issue No. 3, May, 2010.
[19] Samir Kumar Bandyopadhyay, Sarthak Parui, "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.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details