According to the level in which the block falls embedding is done. Blocks with higher difference value will fall in higher level and will be embedded with more number of bits than blocks under other two levels. This implements the idea that more bits of edge pixels can be used to embed data than other pixels. After embedding, if level of a block is distorted then value of pixel is modified in such a way that level remains same. This provides high fidelity stego image. Main drawback of this method is that range table used at sender end is also needed to send to receiver for extraction [13]. In order to overcome the main drawback of edge adaptive steganography [13], a new method has been introduced in 2009 named as variable rate steganography using neighbor pixel relationship. This technique also overcomes the drawback PVD technique [14] which also uses range table. The pixel's relationship with its neighborhood is used to decide whether it is an edge pixel or smooth area pixel. On the basis of neighborhood relationship three methods "four neighbors method", "diagonal neighbor method", "eight neighbor method" were given. All these methods have better Peak signal to noise ratio (PSNR). But main drawback is that only half numbers of the pixels are used for embedding rather than using almost all pixels [15].

In 2010, to enlarge the embedding capacity with high PSNR rate, a new technique has been introduced using hybrid edge detection. Hybrid edge detector is combination of canny edge detector [16] and fuzzy edge detector. Combination of both these detectors provides more number of edge pixels than that of their individual results. In this method after getting edge pixels using hybrid detector image is divided into non overlapping block of size say n. LSBs of first pixel in each block is used to describe the status of other pixels in the block i.e. edge pixels or a non-edge pixels. Edge pixels are embedded with the more number of bits than the non-edge pixels. This method resist statistical analysis based attack as data is not hidden in all the pixels. Beyond providing high embedding capacity higher PSNR is also ensured by this method [16].

In 2011, a new edge embedding technique has been introduced that target on higher PSNR rather than higher embedding rate. This method provides better PSN than [17,16]. Edges of the image are obtained using sobel/canny edge detector. Only horizontal edges of a particular edge length are used further. These edge pixels are used for embedding purpose but to calculate the difference of these edge pixels with upper edge boundary. If this difference is greater than some predefined difference then these upper boundary pixels are used for embedding data bits accordingly. In this way the stego image with least perceptual transparency is obtained. The strong point of this method is high PSNR value but having a drawback of least embedding capacity. Another drawback is that it uses horizontal direction edge pixel boundary only [18].

In 2012, a new parameterized canny edge detection based embedding approach has been introduced. Parameterized canny edge detector uses three parameters i.e. higher threshold value, Gaussian filter and lower threshold value. The value of all these three parameters are user defined. This property makes the stego image more robust as different values of these parameters yields different outputs. In this approach three LSBs of all three channels of edge pixels are replaced with the secret data bits. The advantages of this approach are imperceptibility and irrecoverability [19].

In 2013, to improve the capacity and PSNR new LSB based edge embedding technique using hybrid edge detection filter. Rather than applying Canny with fuzzy edge detector as in [16] combination of the Canny and enhanced Hough edge detector is used to get edge pixels. Message to be embedded is encrypted with AES to provide another level of security. The encrypted message bits are hidden in the smooth area pixels and edge area pixels. For hiding the message bits in smooth area adaptive LSB Substitution technique has been used. Whereas for hiding message bits in the edge area two components-based LSB Substitution techniques has been used.

This method ensures the higher PSNR value and high embedding capacity. Also this method provides security against various attacks e.g. visual analysis, histogram analysis, chi-square and RS analysis [20].

4. Steganography Blended with Cryptography

There are many aspects to security and many applications. One essential aspect for secure communications which is needed with steganography is cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. There are some specific security requirements [30] for cryptography, including Authentication,

Privacy / confidentiality, and Integrity Non-repudiation. The three types of algorithms are described:

(i) Secret Key Cryptography (SKC):Uses a single key for both encryption and decryption
(ii)Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
(iii)Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

Steganography is the other technique for secured communication. It encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Information can be hidden in images [21], audio, video, text, or some other digitally representative code. Steganography systems can be grouped by the type of covers [30] used (graphics, sound, text, executables) or by the techniques used to modify the covers

a) Substitution system
b) Transform domain techniques
c) Spread spectrum techniques
d) Statistical method
e) Distortion techniques
e) Cover generation methods

Spatial domain:

These techniques use the pixel gray levels and their color values directly for encoding the message bits. These

techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image. Moreover these embedding algorithms are applicable mainly to lossless image-compression schemes like TIFF images. For lossy compression schemes like JPEG, some of the message bits get lost during the compression step.

A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method schemes like JPEG, some of the message bits get lost during the compression step.

Transform domain:

These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in the transform domain is widely used for robust watermarking. Similar techniques can also realize large capacity embedding for steganography. Candidate transforms include discrete cosine Transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT). By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. For example, we can perform a block DCT and, depending on payload and robustness requirements, choose one or more components in each block to form a new data group that, in turn, is pseudo randomly scrambled and undergoes a second - layer transformation Modification is then carried out on the double transform domain coefficients using various schemes. These techniques have high embedding and extraction complexity. Because of the robustness properties of transform domain embedding, these techniques are generally more applicable to the “Watermarking” aspect of data hiding.

5. Related Work

A. LSB + Playfair + AES

K Boopathybagan[22] proposed in order to provide strong security, we use two levels of data encryption. When the data encryption is done, using steganographic techniques the cipher text is hidden inside the image. The message will be first encrypted using the Playfair cipher which is also known as playfair square. The first ciphertext will again be encrypted using Advanced Encryption Standard technique LSB encoding is a method in which we hide the data inside an image. The key for data hiding inside image is obtained by the property of image. The property that was used in the reference matrix was to calculate the width to height ratio of the image and decide the key depending on it. Different keys are matched to different height to width ratio. The matrix has different keys based on this ratio. Two levels of data encryption provide increased strength. In transferring secret message, two keys are used: One for the purpose of data encryption. Second key is obtained from the matrix based on the property derived out of the image itself.

B. Modified BPCS + DES + RSA

Vanita M. Mane [23] used and hybrid encryption algorithm, DES algorithm for data transmission because of its higher efficiency in block encryption, and RSA algorithm for the encryption of the key of the DES because of its management advantages in key cipher. Under the dual protection with the DES algorithm and the RSA algorithm, the data transmission will be more secure. The proposed system works to hide data which should not be loss single digit. The proposed method based on JAR. JAR stands for Java Archive and it used to aggregate many Java class files and associated metadata and resources (text images and so on) into one file to distribute application software or libraries on the Java platform. The BPCS (Bit Plane Complexity Segmentation) technique is used to embed data into bitmap files. The ultimate goal is to embed as much data as possible into a cover image without detection by human perception or statistical analysis. In BPCS, the noisy region of an image is located on each bit-plane as small pixel blocks which have noisy patterns.

C. Hash LSB + RSA

Anil Kumar [24] presented the problem statement consisting of embedding the secret message in the LSB of each RGB pixels value of the cover image. Before embedding, the secret message is to be converted to cipher text using RSA algorithm to enhance the secrecy of the message. In this approach we implemented a technique called Hash-LSB derived from LSB insertion on images. Our research has focused on providing a solution for transferring and sharing important data without any compromise in security. All the reputed organizations while sending business documents over the internet always use encryption of the data to protect leakage of information about their organization from their rivals or intruders. We have used Hash-LSB and RSA algorithm to create a secure steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending the data. This technique also applies a cryptographic method i.e RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images.

D. LSB + AES

Ayasha Siddiqa [25] considered a digital color image consists of different pixels. As a colored pixel can be represented as a mixture of red, green and blue color with appropriate proportions. In binary notation, it is represented by a stream of 8 bits. Therefore in total, 24 bits are required to denote a pixel. Thus an image is an array of many bytes each representing a single color information lying in a pixel. In the proposed method, a group of three sequential bytes from such an array is used to embed a bit of the entire message.

The proposed technique has two main parts:

i. Changing the secret message (plain text) to cipher text by AES Cryptography
ii. Hiding the cipher into image by a proposed Steganographic technique 128 bits AES cryptographic algorithm takes a password and encrypts the plain text to cipher text.

This cipher text will be embedded into a cover image using our Steganographic technique. In the Steganographic technique, a filtering algorithm has been used to hide the information. The MSB bit specify the area where to embed the secret message. Our algorithm has the concept of randomly select an image and find if it is a darker or lighter image. Lighter image means MSB bits of Red, Green, and Blue component of a pixel contain at least 2 bit 1's and darker image means MSB bits of Red, Green, and Blue component of a pixel contain at least 2 bit 0's. If lighter pixel is greater than darker pixel, we select lighter pixel area to embed message and vice versa. This proposed work gives more security but provides less capacity for embedding information.

6. Applications

There are many applications for digital steganography of images, including copyright protection, feature tagging, and secret communications [26].

Copyright Protection: A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property [27]. This is the watermarking scenario where the message is the watermark [27]. The "watermark" can be a relatively complicated structure. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified [28]. Detection of an embedded watermark is performed by a statistical, correlation, or similarity test, or by measuring other quantity characteristic to the watermark in a stego-image. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent surge of interest in digital steganography and data embedding.

Feature Tagging: Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features. In an image database, keywords can be embedded to facilitate search engines. If the image is a frame of a video sequence, timing markers can be embedded in the image for synchronization with audio. The number of times an image has been viewed can be embedded for "pay-per-view" applications.

Secret Communications: In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use steganography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers or eavesdroppers.

7. Conclusion

By this survey paper reader can get deep understanding of what is steganography. It is analyzed that it is impossible to stop and detect the threats completely. As steganography is widespread, but alone it is not sufficient for hiding a secret message. So for this requirement, cryptography is combined with steganography to archive the same.

References

[1] A.Joseph Raphael, Dr.V Sundaram, "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630 ISSN:2229-6093.
[2] Gandharba Swain, Saroj Kumar Lenka,"A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels", Proceedings of the International Conference on Communication and Computational Intelligence – 2010, Kongu Engineering College, Perundurai, Erode, T.N.,India.27 – 29 December,2010.pp.529-534.
[3] Ronak Doshi,Pratik Jain,Lalit Gupta," Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645.
[4] Richard Bergmair ,"Towards Linguistic Steganography: A Systematic Investigation of Approaches, Systems, and Issues Oct-03 – Apr-04.
[5] Richard Bergmair. 2007 A comprehensive bibliography of linguistic steganography. In Proceedings of the SPIE Conference of security. Steganography and watermarking of multimedia contents, 6505.
[6] L. Y. POR, B. Delina, ""Information Hiding: A New Approach in Text Steganography", 7th WSEAS Int. Conf. on applied computer & applied computational science (ACACOS '08), Hangzhou, China, April 6-8, 2008.
[7] A. Shaddad, J. Condell, K. Curran, and P. Mckevtt., "Biometric inspired digital image steganography," Proceedings of 2008 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, pp. 159-168, 2008.
[8] Mohammad Ali Bani Younes, Aman Jantan, A New Steganography Approach for Image Encryption Exchange by using the LSB insertion, International Journal of Computer Science and Network Security, Vol 8, No 6 , pp. 247-254, June 2008.
[9] Mohammad Ali Bani Younes, Aman Jantan, A New Steganography Approach for Image Encryption Exchange by using the LSB insertion, International Journal of Computer Science and Network Security, Vol 8, No 6, pp. 247-254, June 2008.
[10] Ross J. Anderson, Fabian A.P. Petitcolas, On The Limits of steganography, IEEE Journal of selected Areas in communication, 16(4), pp. 474-481, May 1998.
[11] Kathryn Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Steganography", Proceedings of the Computing Women's Congress, 2006.
[12] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Proceedings of 2005 Instrument Electric Engineering, Vis. Images Signal Process, vol. 152, no. 5 pp. 611–615, 2005
[13] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung- Min Sun, "Adaptive Data Hiding in Edge Areas

of Images with Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, pp. 488-497, 2008
[14] D. C. Wu and W. H. Tsai, "A Steganographic method for images using pixel value differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003
[15] Hossain, M. Al Haque and S. Sharmin, F., "Variable rate Steganography in gray scale digital images using neighborhood pixel," 12th International Conference Dhaka, Information Computers and Information Technology, ICCIT '09, pp. 267- 272, Dec 2009
[16] Wen-Jan Chen a, Chin-Chen Chang, T. Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications, vol. 37, pp. 3292–3301, 2010
[17] Hossain, M. Al Haque and S. Sharmin, F., "Variable rate Steganography in gray scale digital images using neighborhood pixel," 12th International Conference Dhaka, Information Computers and Information Technology, ICCIT '09, pp. 267- 272, Dec 2009.
[18] Hussain, M. and Hussain, "Embedding data in edge boundaries with high PSNR," Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6, Sept 2011
[19] [19]Youssef Bassil, "Image Steganography Based on a Parameterized Canny Edge Detection Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 60, no. 4 2012
[20] Mamta Juneja and Parvinder S. Sandhu, "A New Approach for Information Security using an Improved Steganography Technique," J Inf Process Syst, vol. 9, no. 4, 2013
[21] Chandramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003
[22] S Ushll, G A Sathish Kumal2, K Boopathybagan, "A Secure Triple Level Encryption Method Using Cryptography and Steganography" 20 II International Conference on Computer Science and Network Technology
[23] Smita P. Bansod Vanita M. Mane Leena R. Ragha, "Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India
[24] Anil Kumar, Rohini Sharma," A Secure Image Steganography Based on RSA Algorithm and Hash-LSB TechniqueInternational Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013 ISSN: 2277 128X
[25] Md. Rashedul Islam1, Ayasha Siddiqa2, Md. Palash Uddin3, Ashis Kumar Mandal4 and Md. Delowar Hossain5 "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", 3rd International Conference on Informatics, Electronics & Vision 2014
[26] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, pp. 26-34, February 1998., 4. W Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, No. 3 and 4, pp. 313-336, 1996
[27] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia data embedding and watermarking technologies," Proceedings of the IEEE, Vol. 86, No. 6, pp. 1064-1087, June 1998., 6. R. Wolfgang, C. Podilchuk and E. Delp, "Perceptual watermarks for images and video," to appear in the Proceedings of the IEEE, May, 1999
[28] R. B. Wolfgang and E. J. Delp, "Fragile watermarking using the VW2D watermark," Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents, SPIE Vol. 3657, San Jose, CA, January 1999
[29] Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the unseen" IEEE transaction on Computer Practices. 1998
[30] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002
[31] D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995. ISBN: 0849385210