AN INTRODUCTION OF DIGITAL IMAGE STEGANOGRAPHY TECHNIQUES: AN OVERVIEW

[1]Shweta Agrawal, [2]Dr. Neha Singh
[1]M. Tech. Scholar, Department of Computer science engineering, Acropolis Institute of Tech.& Research Bhopal, M.P., India
[2]Associate Professor, Department of Computer Science Engineering Acropolis Institute of Tech. & Research Bhopal, M.P., India

Abstract: ***Transmitting confidential images between two channels experience the ill effects of hacking. Thusly, ensuring confidentiality has turned into an extremely essential issue. As of late, a few techniques are produced to secure vital information. The principle thought depends on embedding imperative information in sight and sound carrier for example, text, image, sound, and video. The created techniques might be appointed steganography and watermarking. Steganography expects to embed huge measure of secret information in mixed media carrier while watermarking expects to concealed little measure of secret information in sight and sound carrier. In this paper we have survey on the different stegaongraphy approach and also covered a comparative study among them, and we analyzed that hybrid approach is better than another approach.***

Index Terms - Steganography, Embedding, Conceal, Information Hiding, DWT, LSB.

I. INTRODUCTION

Now days, the communication is the basic necessity of each developing zone. Everybody wants the secrecy and safety of their communicating information. In our everyday life, we use numerous secure pathways like web or phone for transferring and sharing information, yet it's not safe at a specific level. With a specific end goal to share the information in a hid way two techniques could be used. These mechanisms are cryptography and steganography. In cryptography, the message is altered in an encrypted form with the assistance of encryption key which is known to sender and receiver as it were. The message can't be accessed by anybody without using the encryption key. Regardless, the transmission of encrypted message may effectively excite attacker's Suspicion and the encoded message may therefore be captured, attacked or decoded brutally. To beat the weaknesses of cryptographic strategies steganography systems have been made. Steganography is the craftsmanship and science of communicating in such a way that it hides the existence of the correspondence. Thus, steganography hides the existence of information so that nobody can recognize its presence. In steganography the process of concealing information content inside any interactive media content like image, sound, video is referred as a ―Embedding.

II. STEGANOGRAPHY

Steganography is the act of hiding a record, message, image, or video inside another file, message, image, or video. The word steganography combines the Greek words steganos, signifying "covered, concealed, or ensured", and graphein signifying "writing".

III. IMAGE STEGANOGRAPHY

Image steganography concerns with hiding secret information in digital images. There exists a large variety of image steganography techniques. Some of these techniques are more complex than the others, and all of them have respective strong and weak points. Image steganography techniques can be classified into spatial domain (image domain) steganography, transform domain (frequency domain) steganography, spread spectrum steganography and mode based steganography. Figure 1 shows an order tree of image steganography systems. The accompanying areas depict the different methods for image steganography.

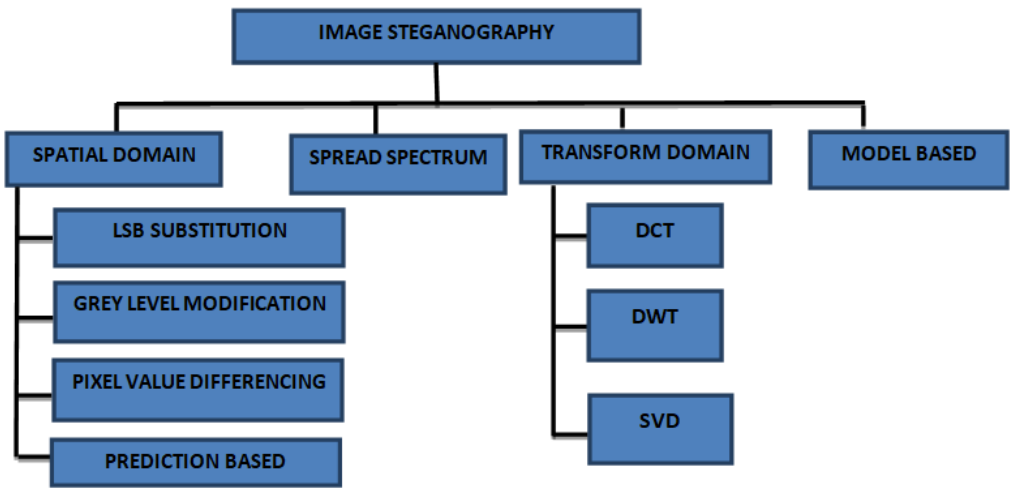

Figure 1. Classification of Image Steganography technique

3.1 Spatial Domain Methods

Image domain applies bit insertion and noise control of a secured image. In spatial domain steganography, embedding the secret message will be done to the pixels straight forwardly, for instance, Least Significant Bit (LSB), gray level adjustment, pixel value differencing, quantization index modulation, multiple base notational system, and prediction based.

3.1.1 LSB Substitution

LSB is a simple and basic technique for covering information on cover image. Digital images can be classified as grayscale (8-bit-planes) or colored (24 bit planes) which depends on every pixel intensity levels, i.e., every pixel can be represented by 24-bits, 8-bits or indeed, even just a single piece. On the off chance that each pixel of the digital image is assumed as n bits then the digital image can be composed of n numbers of 1-bit planes in the range from bit-plane zero to bit-plane n-1. For instance, in a gray scale image every pixel is represented by eight bits, so the image can be sliced onto eight slices (bit planes) from bit- plane zero to bit-plane 7.These eight slices are isolated onto two parts: Most Significant Bits (MSE) and Least Significant Bits (LSB). LSB don't hold visually critical information, so that is the ideal condition for embedding watermark bits. In this strategy, the process of embedding depends on choosing a subset of cover image and applying the substitution activity on them. That exchanges the LSB of cover image by the watermark. The LSB strategy is portrayed by simplicity, high limit, easy to understand and actualize, and can't be seen by the stripped eye. Nevertheless, the limitations of this method are that less robust (Easy control by assailants), vulnerable to noise, scaling and trimming

3.1.2 Gray Level Modification

This technique maps information by modifying gray levels of the pixels without embedding or on the other hand hiding it and utilizations the origination of even and odd numbers in mapping the information in the cover image. For case, even qualities are mapped with zero and odd values are mapped with one. The gray level change strategy is portrayed by low computational complexity and high capacity.

3.1.3 Pixel Value Differencing

In 2003, Da-Chun et al. built up another embedding technique, called Pixel Value Differencing (PVD), in light of the difference between pixel values. First, they separate the cover image into non-covering squares having two interfacing pixels. At that point, they change each square difference. They found that the bigger the difference into unique pixel esteem, the more noteworthy the change will be. They likewise found that the installed mystery bits number relies upon the pixel case that will be in smooth zone or in edge zone. In smooth region, the difference between adjoining pixels is less while in edge region it is more. Along these lines, the information that is inserted into edge zone pixels is more than installed into smooth zone. This procedure is superior to LSB in watermarked image quality and imperceptibility.

3.1.4 Prediction Based Steganography

A scheme in light of prediction based steganography is produced. The predictive coding approach is acquainted as an answer with the issu of stego image distortion (which originated from embedding information by altering the estimations of the pixel straight forwardly), as 'prediction based steganography' predicts pixel esteems utilizing an indicator which gauges input image pixel values. The prediction based steganography procedure is characterized by high payload capacity. This plot shroud tree demonstrated unrivaled with about 99.85% capacity of embedding.

3.2 Transform Domain Technique

Transform Domain applies image transformation and control of calculation. In transform area steganography, installing the secret requires transforming the image from the spatial area to the recurrence area by utilizing any of the transforms, for illustration, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Single Value Decomposition (SVD). After the transformation process, the installing procedure will be done in legitimate transform coefficients.

3.2.1 Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) depends on changing sign or image from spatial space to frequency area. The DCT split the image as appeared in figure 2 up to otherworldly sub-groups (parts) of various note worthiness regarding the visual nature of the image. Embedding positions Choices: (I) Low frequency coefficients: Bad invisibility, since human eye is delicate to clamor on it, as it contains the image visual parts, (ii) High-frequency coefficients: terrible vigor, as the image could be debased through commotion assaults or pressure, and (iii) Middle-frequency coefficients: great invisibility and power, so it is the best choice. The DCT is characterized by the most vigorous procedure to lossy pressure and Image visibility is ensured. In any case, the disadvantages of this strategy are that Block effect Picture cropping effect.

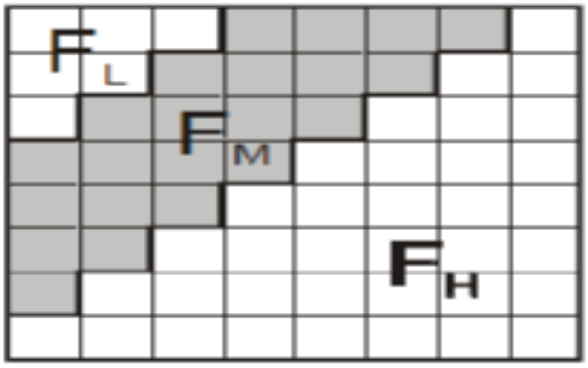

Figure 2. Discrete Cosine Transform (DCT)

3.2.2 Discrete Wavelet Transformation

Wavelet change is utilized as a part of a wide range in signal processing applications and image pressure. It isolates the signal to set of fundamental capacities which are called wavelets. Discrete Wavelet Transform (DWT) is described as an effective and exceptionally adaptable technique for breaking down signals sub bands. In instance of one-dimensional DWT, image is deteriorated into 4 bands signified by Low-Low (LL) level, High-Low (HL) level, Low-High (LH) level and High-High (HH) level, as appeared in Figure 3. Where, H symbolizes high-pass channel (High frequency) and L symbolizes low-pass channel (Low frequency).In instance of Multi-Level Discrete Wavelet Transform, as appeared in Figure 3. This speaks to the image in the wake of applying three times of DWT. The image comprises of frequency zones of LL1, LH1, HL1, HH1. The LL1 (low frequency zone) is disintegrated onto sub-level frequency region data of LL2, LH2, HL2, HH2. By applying past decay over and over the image can be disintegrated onto N level wavelet transformation. The DWT is characterized by Imperceptibility and Robustness. In any case, the downsides of this strategy are that Long pressure time, High computational cost, Noise/obscure near edges of images.

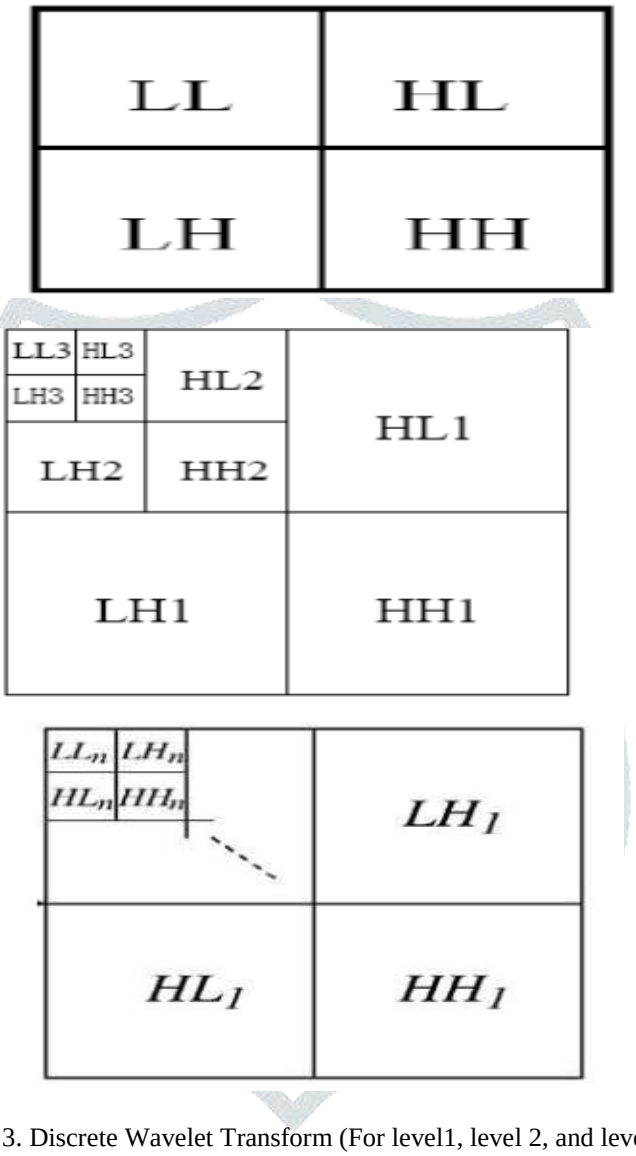

Figure 3. Discrete Wavelet Transform (For level1, level 2, and level N)

3.2.3 Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) is a mathematical technique based on a linear algebra theorem which declares that the rectangular matrix (A) can be analyzed into three matrices: U (Orthogonal matrix), S (Diagonal matrix), and V (Transpose of an orthogonal matrix). The theorem is presented usually like: $A = USVT$.

3.3 Hybrid Technique

A few analysts join at least two methodologies of the past techniques to strategy another technique. Because of this blend, the hindrances of one technique will be expelled as a result of the impact the other utilized technique. In this way, the hybrid techniques are superior to individual past techniques. A hybrid watermarking technique consolidated delicate and robust techniques is acquainted with make strides confirmation, check, respectability and copyright security at the same time. A hybrid DWT-SVD technique is proposed by utilizing human Visual System Display and contrasted and SVD as it were. The examination demonstrated that the hybrid strategy is better in PSNR and BCR (Bit Correlation Rate).A hybrid DCT-SVD technique is proposed for copyright insurance. This strategy is more robust, likewise accomplishes better PSNR and correlation. A hybrid technique joined of DWT, DCT and SVD is Proposed and contrasted and that utilized just DWT and that utilized DCT and SVD. The examination demonstrated that the hybrid technique is better in PSNR and connection. A hybrid strategy joins the three techniques DCT, DWT and SVD is displayed and discovered that the comes about are moved forward. A hybrid technique joins DWT and DCT is proposed while a hybrid technique which joins DWT and SVD is created. The PSNR esteem was moved forward what's more, the robustness was high. A hybrid technique joins DWT, DCT and SVD is proposed. The test comes about demonstrate that the image can overcome JPEG lossy compression and cropping of an image.

IV. RELATED WORK

Research on computerized steganography is going ahead since in excess of two decade, but the indication of steganography can be seen from old days also. If we discuss advanced steganography, before analysts were working on text steganography i.e. concealing text information into a text document .After that they began working on image and audio steganography .From 5 to 6 years work on video steganography is going on and the idea of network steganography and protocol steganography is new one[2].

The practicality of the proposed strategies has been surveyed by preparing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). Steganography is the workmanship and examination of making secured messages to such a degree, to the point that nobody, close to the sender and proposed beneficiary, associates the proximity with the message, a sort of security through uncertain quality. It is thusly a book on charm. It is creating in its zenith since it doesn't pull in anyone autonomous from any other person. In this paper a similar examination of two or three approaches has been satisfactorily acknowledged and happens are passed on. The MSE what's more, PSNR of the amazing number of techniques are also looked other than this paper showed a foundation talk and use on the significant figuring's of steganography sent in automated imaging. The rising frameworks, for example, LSB based, OPAP, Altered case based LSB utilizing MSE, Inverted outline based LSB utilizing Relative entropy, String of 1 and 0 based, mod based what's more, Mod 10 Generally few of these approaches have a tendency to have a lower payload emerged from spatial territory computations.[1].

This paper displays a definite depiction of another protected Block Permutation Image Steganography (BPIS) calculation. The calculation changes over the secret message to a twofold arrangement, partitions the paired grouping into pieces, permutes the square utilizing a key-based haphazardly produced change, links the permuted squares framing a permuted double grouping, and afterward uses the Least-Significant-Bit (LSB) way to deal with implant the permuted twofold succession into BMP image record. The calculation execution is explored through playing out various investigations, and for each try the PSNR (Peak Signal-to-Noise Ratio) between the stego and cover images is figured. The comes about demonstrate that the calculation gives high image quality, and imperceptibility, and above all higher security as secret can't be recuperated without knowing the stage, which has a many-sided quality of O(N!), where N is the length of the stage[3].

This paper proposes a productive technique for creating computerized watermark from biometric iris is extraordinary and can be considered to demonstrate possession. The issue of advanced watermark is owed in this. The biometric example of the iris image is utilized to create the computerized watermark having a cradle property [4].

V. COMPARITIVE STUDEY

Table 1. Comparison between spatial domain techniques and transform domain techniques

Domain / Factor	Spatial	Transform
Embedding	Directly onto image pixels	On transform coefficient
Imperceptibility	Highly controllable	Lower controllable
Capacity	High	Low
Robustness	Low	High
Complexity	Low	High
Processing time	Low	High

VI. CONCLUSION

As we discussed that since two decades we came through numerous kinds of steganography and the network steganography, protocol steganography, steganography on web are the better and brighter one including technique like DCT, DWT, data hiding, masking, and any suitable calculation is utilized to install the secret information in the cover file. Every one of these algorithms endeavor to fulfill three most imperative variables of steganographic plan i.e. un-perceptibility, robustness, and limit. At that point, some hybrid techniques are examined. In future embedding limit can be significantly upgraded and can have the capacity to withstand against a wide range of attacks. This technique can be reached out to embed audio and in addition video for secure sight and sound transmission.

REFERENCES

[1] R.Amirtharajan, R.Akila, P.Deepika Chowdavarapu "A Comparative Analysis of Image Steganography", International Journal of Computer Applications (0975 – 8887) Volume 2 – No.3, May 2010.

[2] M.S.Subhedar and V.H. Mankar,"Current Status and Key Issue in Image Steganography;A survey", Computer Science review,Vol. 13-14,pp.95-113,2014.

[3] Hussein Al-Bahadili,"A Secure Block Permutation Image Steganography Algorithm", (IJCIS), Vol.3, No. 3, September 2013.

[4] Dutta, M.K., Singh A. and Zia, T.A., "An Efficient and secure digital image watermarking using features from iris image", IEEE 2013, pp451-456[11]

[5] Alaa Fkirin, Ayman El-Sayed, Gamal Attiya," Steganography Literature Survey, Classification and Comparative Study",CAE-USA, Volume 5 – No.10, September 2016

[6] Ngatia E., W. & Njuguna A. (2018), "Information Security through an Improved Image Steganography Algorithm", Journal of Information and Technology Vol 1(1) pp. 28-46.

[7] K B Shiva Kumar, K B Raja, Sabyasachi Pattnaik," Hybrid Domain in LSB Steganography", International Journal of Computer Applications (0975 – 8887) Volume 19– No.7, April 2011.