A Survey on Various Techniques of Image Data Cryptography Techniques and Features

M. Tech. Scholar Arzoo Singh  
Dept. of Electronic & Communication  
Sagar Institute of Research and Technology  
Bhopal, Madhya Pradesh, India  
arzoo.singh1608@gmail.com

Prof. Abhishek Sharma  
Dept. of Electronic & Communication  
Sagar Institute of Research and Technology  
Bhopal, Madhya Pradesh, India

Abstract - With the increase in the digital media transfer and modification of data is very easy. So these works focus on transferring data by hiding in image. So maintain the image quality is done by Digital image processing on various issues. This paper gives a brief survey of image data cryptography techniques for various environmental scenes. Image analysis features are described in this paper with these requirements. As hiding data is small but it goes under some kind of attacks which are also cover in this paper as they are the best measure for comparing different techniques of data hiding.

Keywords- Digital data hiding, Encryption, Histogram, Image Processing.

I. INTRODUCTION

As web is developing definitely clients are draw in by different specialist organizations step by step. Some of online shops, computerized show casing, informal organization and so on. This simple access prompt change the proprietorship effectively, as clients can stolen other work and make computerized print with there name. In any case, this innovation offer ascent to new issue of piracy. To conquer this issue numerous approaches were recommended and restrictive of the advanced information is protected. So to defeat this distinctive strategies are use for safeguarding the restrictive of the proprietor.

Out of many methodologies advanced information inserting which is otherwise called computerized Data Hiding assumes a critical part. Keeping in mind the end goal to give proprietership of the information proprietor, advanced information was implanted into the image, video, or information as in [1, 2, 4]. One of the real fundamentals of information hiding is that the hidden information must be hazy. The utilization of stenography has many points of interest and are extremely helpful in computerized picture handling which makes them appropriate for a wide collection of uses. In this cutting edge region, digital incredible comfort in transmitting a lot of information in various parts of the world.

In any case, the wellbeing and security of long separation correspondence remains an issue. Keeping in mind the end goal to take care of this issue of security and wellbeing has prompted the advancement of stenography plans. Stenography is not quite the same as watermarking and cryptography.

The fundamental target of stenography is to conceal the presence of the message itself, which makes it troublesome for a spectator to make sense of where precisely the message is. Then again, cryptography systems have a tendency to secure correspondences by changing the information into a frame with the goal that it can't be comprehend by a meddler. Also, in watermarking logo is more critical than data. Stenography is the sort of concealed correspondence that signifies "secured expressing" (from the Greek words stego or "secured" and graphos or "to write").

Information hiding is the procedure to cover information inside a cover media. In this way, the information concealing procedure contains two sorts of information, embedded information and cover media information. The information is transmitted by implanting it inside Images, which enhances information security. The information concealing strategy in which the reversibility can be accomplished is called Reversible information hiding.

This method is used to enhance the security of the cover Image in encryption. Reversible image data hiding (RIDH) is one strategy for information concealing procedure, which ensures that the cover picture is recreated flawlessly after the extraction of the implanted message. The reversibility of this technique makes the information concealing methodology attractive in the basic situations, e.g., military and remote detecting, law crime scene investigation, medical picture sharing and copyright confirmation, where the original cover picture is required after remaking.
II. RELATED WORK

In [4] digital information was embedded in the chosen bit of the picture where edge locale was select for inserting. Here paper has build up a new approach of discovering pixel representing to edges. By using Dam and BCV approach picture was section into edge and non edge locale. One disadvantage of this work was there where picture should be in binary format only. With above issues picture was exceptionally strong against various sort of attackss like channel, noise, and so forth.

In [5] author has expand the work done in [4] by expanding the general limit of the implanting information space. Here in Dam and BCV method author begin taking a pixel value at the encompassing region of the edge area pixel. So general limit of the information covering up was radically increment in this paper. Here even of hiding more information inserted picture was vigorous against various kind of attacks too.

In [7] self inserting idea was proposed by the authors where picture itself produce the information for hiding while to secure information in organize fountain codes were produced for lost data recovery. As in fountain codes more than one required bundle were send in network which help in recovering the missed or degenerate information packets. Here work has extraordinary confinement was that subsequent to implanting the picture isn't accessible in unique arrangement before extraction. So principle reason for this work is for exchanging the information parcel from sender to collector as it were.

In [6] same idea of picture Data Hiding self age was done, here picture was utilize to the point that it produce its own particular Data Hiding. This paper concentrate on the picture improvement where spatial region was use for embeddings the digital information as a carrier object. In the meantime comparative data was required at the beneficiary which help in finding the digital information back. Be that as it may, to cover both intra-codeblock and between codeblock strategy is use.

In [8] author embrace KSVD procedure for hiding the digital information. Here by using the RCS calculation encryption of the digital information was finished. Here one word reference was kept up at the collector and transmitter end for lessening the measure of transporter flag. In this work in the wake of inserting some vacnt space between the information was use for the information hiding. This work has give flexibility for extraction of picture or digital information or both in any request.

In [12] authors utilize the DWT feature for finding the pixel value for embedding. While in order to increase the randomness in the embedding the selection of image was not sequential but it would utilize the random Gaussian function for selecting pixel of different position. At the receiver side with the help of some supporting information it was found that Data Hiding was extract from the image. Here it was obtained that both Data Hiding and image got reverse at the receiving end.

III. FEATURES FOR IMAGE CRYPTOGRAPHY

As Image is collection or sequence of pixel and each pixel is treat as single value which is a kind of cell in a matrice. In order to identify an object in that image some features need to be maintained as different object have different feature to identify them which are explain as follows:

1. Color feature- Image is a matrix of light intensity values, these intensity values represent different kind of color. so to identify an object color is an important feature, one important property of this feature is low computation cost.

Fig. 3 Represent the HSV (Hue Saturation value) format of an image.

Different Image files available in different color formats like images have different colur format ranging from RGB which stand for red, green, and blue. This is a three dimensional representation of a single image in which two dimensional matrix represent single color and collection of those matrix tends to third dimension. In order to make intensity calculation for each pixel gray format is use, which is a two dimension values range from 0 to 255. In case of binary format which is a black and white color matrix whose values are only 0 or 1. With the help of this color feature face has been detected efficiently in [8].
2. **Edge Feature** - As image is a collection of intensity values, and with the sudden change in the values of an image one important feature arises as the Edge as shown in figure 4. This feature is used for different types of image object detection such as building on a scene, roads, etc [7].

There are many algorithms developed to effectively point out all the images of the image or frames which are Sober, pewit, canny, etc. out of these algorithms, canny edge detection is one of the best algorithms to find all possible boundaries of an image.

![Fig. 4 Represent Edge feature of an image.](image)

3. **Texture Feature** - Texture is a degree of intensity difference of a surface which enumerates properties such as regularity and smoothness [6]. Compared to color space model, texture requires a processing step. The texture features on the basis of color are less sensitive to illumination changes as same as to edge features.

4. **Corner Feature** - In order to stabilize the video frames in case of moving camera it require the difference between the two frames which are point out by the corner feature in the image or frame. So by finding the corner position of the two frames one can detect resize the window in original view. This feature is also used to find the angles as well as the distance between the object of the two different frames. As they represent point in the image so it is use to track the target object.

![Fig 5 Represent the corner feature of an image with green point.](image)

**IV. WATERMARK ATTACKS**

As video move from one place to another by a network. So movement of video makes various changes in the original data. So it is required that data hiding or data hiding technique should be robust against various attacks which is described in following points.

1. **Noise Attack** - This is very common problem in the transfer channel where information is send in the data consist of some other information. So merging with other data cause small change in data which is term as noise in the original signal. In experiment different noise producing function is use for adding these noise in the data such as: Gaussian Noise Attack, Salt & Pepper Noise, Speckle Noise Attack, etc.

2. **Filter Attack** - In this type of attack as different servers act as the mediator for passing the information from sender to receiver end so filter use in those server make few changes in the data. This is term as filter attack. In experiment same type of attack is done by applying the filters such as average filter, motion filter, sharpen filter, etc [6,7].

3. **Compression Attack** - In various case when data is compress for different requirement information hide in the video get loss. So algorithm should be protective against such type of compression attacks. Some time due to change in video format different compression algorithm use different frame compression technique [7]. Some filtering attacks are: MP4 compression, MPEG compression, etc.

4. **Scene Swapping** - This is count as temporal attack where video frame are swap with its own frame. In this type of attack correlation between the watermark extraction get loss and extracted frame get highly
affected so data hiding algorithm which was depend on frame sequence is not robust against this attack.

V. EVALUATION PARAMETERS

1. Peak Signal to Noise Ratio

$$\text{PSNR} = 10\log_{10}\left(\frac{\text{Max}_{\text{pixel}} \text{value}}{\text{Mean}_{\text{Square}} \text{error}}\right)$$

2. Signal to Noise Ratio

$$\text{SNR} = 10\log_{10}\left(\frac{\text{Signal}}{\text{Noise}}\right)$$

3. Extraction Rate

$$\eta = \frac{n_t c}{256 \times 100}$$

Here n_t is number of pixels which are true.
Here n_c is total number of pixels present in Data Hiding.

4. SSIM - The Structural Similarity Index Module (SSIM) is a perceptual metric that quantifies image quality degradation caused by processing such as data compression or by losses in data transmission. The SSIM index is calculated as,

$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{\mu_x^2+\mu_y^2+C_1(\sigma_x^2+C_2)\sigma_y^2+C_2}$$

Where $\mu_x$: the average of x
$\mu_y$: the average of y
$\sigma_x^2$: the variance of x
$\sigma_y^2$: the variance of y
$\sigma_{xy}$: the covariance of x and y.
$c_1$, $c_2$: two variables to stabilize the division with weak denominator.

The SSIM index satisfies the condition of symmetry: $\text{SSIM}(x,y) = \text{SSIM}(y,x)$

VI. CONCLUSION

With the high demand of image in various fields researchers get attracted for analysis. This paper covers various approaches of image data hiding. As unfavorable weather condition make high data lose, so recovering in those is done by extracting features from the image. It is also obtained that color and edge feature plays an important role for image data hiding. Here frequency based water marking technique is good for invisible embedding, but low data is embedded in the image. In future, work can be improved for other attacks such as geometry of image.

REFERENCES

5. Angela Piper1, Reihaneh Safavi-Naini. “Scalable Fragile Data Hiding For Image Authentication”. Published In 1st Information Security, On 31st December 2012
8. Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, And Xiaojie Guo High Capacity Reversible Data Hiding In Encrypted Images By Patch-Level Sparse Representation. Ieee Transactions On Cybernetics 2015.