*Proceedings of 1st Shri Chhatrapati Shivaji Maharaj QIP Conference on Engineering Innovations*
*Organized by Shri. Chhatrapati Shivaji Maharaj College of Engineering, Nepti, Ahmednagar*
*In Association with JournalNX - A Multidisciplinary Peer Reviewed Journal, ISSN No: 2581-4230*
*21st - 22nd February, 2018*

# A STEGANOGRAPHY IMPLEMENTATION

Miss. Pooja N. Dhawale
Shri Chhatrapati Shivaji Maharaj COE, Nepti Ahmadnagar,

Miss. Prajakta S. Patil
Shri Chhatrapati Shivaji Maharaj COE,Nepti , Ahmadnagar,

Miss. Shubhangi M. Waskar
Shri Chhatrapati Shivaji Maharaj COE, Nepti,Ahmadnagar

**Abstract —**
**Numerous techniques are utilized to hide information in different organizations in steganography. The most broadly utilized system by virtue of its straightforwardness is the utilization of the Least Significant Bit. Least Significant Bit or its variations are typically used to shroud information in a digital image. Alternate bits might be utilized yet it is exceedingly likely that picture would be twisted. This paper talks about the workmanship and investigation of Steganography as a rule and proposes a novel procedure to shroud information in a beautiful picture utilizing minimum huge piece.**
**Index Terms - Stenography, Data hiding, Digital Images, Pixels.**

## I. INTRODUCTION

The Greek word "steganos" which means secured composing is essentially the idea driving the hypothesis of steganography. Here it is hard to try and distinguish that a message is being sent. This kind of figuring called steganography, the old craft of concealing messages sent imperceptible. This technique is picking up fame with ordinary passing in light of its special properties and those days are not far-removed when it would be received by multitudes of the world for mystery message passing. The historical backdrop of sending concealed message is extremely old. Greeks utilized it composing message on some material and later covering it with wax, inking messages on uncovered head, later developing hair to cover it up. In World War II imperceptible inks were utilized to compose messages in the middle of the lines of typical instant message [1]. World War II saw the utilization of microdots by Germans. In microdots innovation, photo of mystery message taken was lessened to size of a period. This innovation was called "the adversary's showstopper of surveillance" by FBI chief J. Edgar Hoover [1]. Ordinary and guiltless messages conveying mystery messages moved starting with one place then onto the next.

The approach of PCs reformed the world. It had its significant effect on all the aspect of life including steganography. PCs encouraged sending and trading photos, welcoming cards, birthday cards and so forth in a way that a great many these are traded on the Internet on regular routine. It isn't just conservative, yet clients can pick cards from a huge assortment of them uninhibitedly accessible and it requires no investment to send them. Moreover, sound and video document are likewise traded unreservedly. This trade of cards and documents has additionally offered quality to steganography. It is unequivocally being accepted by US insight offices that Al-Quida is trading maps of potential focuses using his innovation.

Section II talks about that kind of steganography and the media usage utilized for this system. Section III talks about that in the matter of how the digitalized pictures are developed. Section IV contrasts steganography and cryptography. Section V clarifies different procedures utilized as a part of steganography. Section VI gives out the subtle elements of the proposed system.

## II. TYPES AND MEDIA

Steganography may be classified as pure, symmetric and asymmetric. While pure steganography does not require any trade of data, symmetric and asymmetric needs to trade of keys earlier sending the messages. Steganography is exceptionally subject to the sort of media being utilized to hide the data. Medium being normally utilized incorporate content, pictures, sound records, and system conventions utilized as a part of system transmissions [2].

Image Steganography is for the most part more favored media on account of its safeness and fascination. Also trade of welcome through computerized implies is on the expansion through the expanded utilized of the web and simplicity of solace and adaptability is sending them. Innovation progression in plan of cameras and advanced pictures being spared in cameras and afterward exchange to PCs has additionally improved numerous folds. Furthermore, the instant messages covered up in the pictures does not twist the picture and there are strategies which just irritate just a single piece of a picture effects' identity's relatively immaterial on its quality.

Applications of steganography can be enormous. It can have legitimate use to protect copyrights, to main confidentiality. It can be used by law breakers to pass information which may have highly disastrous effects. One of the significant disadvantages of steganography is that one can cover up next to no data in the media chose. Section III talks about that in the matter of how the computerized pictures are built.

## III. CONSTRUCTION OF IMAGES

An advanced image is "a variety of numbers that speak to light forces at different focuses" [4]. These light powers or pixels are consolidating to frame the picture's raster information. The pictures can be of 8-bits or 24 - bits. In GIF picture size of every pixel is 8 bits. In this arrangement the hues are spoken to from most used to slightest utilized hues [10]. The pictures

with 256 hues and pixel estimation of 640*480 size up to 300 kilobits [6] where as a high determination (1024*768) picture of 24 bits may have measure bigger than 2 megabits. Albeit bigger size document encourages bigger measure of information to be covered up however exchanging bigger size on the web can cause suspicious and additionally require more transfer speed along these lines expensive. Two kinds of record pressure for the most part used to overcome above said issues are Lossy and Lossless compressions. It merits bringing up here that both of these systems utilize isolate components however objective is same that is to lessen the span of record to encourage capacity [6].
JPEG (joint photographic experts group) is a case of lossy pressure. Its leverage is that it spares more space however in doing as such loses its innovation. Then again GIF (graphic interchange format) and BMP (bitmap file) are examples of lossless pressure which is as a rule suggested media writes since both of these hold their innovation [5].

Any image comprise of 3 essential hues in particular red, green and blue, These hues generally known as RGB together shape an advanced picture. As said a picture is for the most part portrayed as number of pixels. Each shade of a pixel comprises of a byte or 8 bits and convey certain data. Data is put away in the primary piece of each progressive pixel. Since data is put away at all critical piece so same does not influence the nature of picture altogether. The entire message is inserted in the picture along these lines and results have indicated scarcely any corruption in the photo quality same strategy might be connected in the video record. It is apropos to say here that this framework is the minimum secure technique as message is inserted in plain content in innocuous pictures to be transmitted to the goals.
However, its security lies in stirring up this picture with concealed message to be transmitted with a great many different pictures sent in their ordinary game-plan. A large number of pictures should be screened to find the coveted picture. It is of foremost significance to choose picture; renowned sketches ought not be chosen, in certainty customary pictures must be picked. By and by BMP pictures of 800*600 pixels are not normally observed on the Internet along these lines its utilization could be suspicious [11]. In 8-bit picture, since pointers to sections in the palette changed, accordingly, change of even one piece is very observable. Dim scale palettes because of minimum articulated shades are [7] prescribed. Area IV contrasts steganography and cryptography.

## IV. STEGANOGRAPHY V/S CRYPTOGRAPHY

Numerous a times Steganography is identified with Cryptography. It might be a deceptive articulation concerning a Steganography approach. Steganography is identified with Cryptography by implying that both are utilized for security purposes yet with various approach or execution. Steganography is, alongside Cryptography, an exceptionally antiquated idea however its application changes as per developing advancements. It is correlated to specify here that both of these advancements may not be taken as opponent to each other but rather they can assume a vital part if these supplement each other. Area V clarifies different procedures utilized as a part of steganography.

## V. TECHNIQUES

The three fundamental strategies utilized for Steganography are: [3]

- Injection: Hiding information in areas of a document that are disregarded by the preparing application. Along these lines abstain from adjusting those record bits that are important to an end-client leaving the cover document impeccably usable.
- Substitution: Replacement of the slightest critical bits of data that decide the significant substance of the first document with new information in a way that causes minimal measure of bending.
- Generation: Unlike infusion and substitution, this does not require a current cover record but rather creates a cover petition for the sole motivation behind concealing the message.

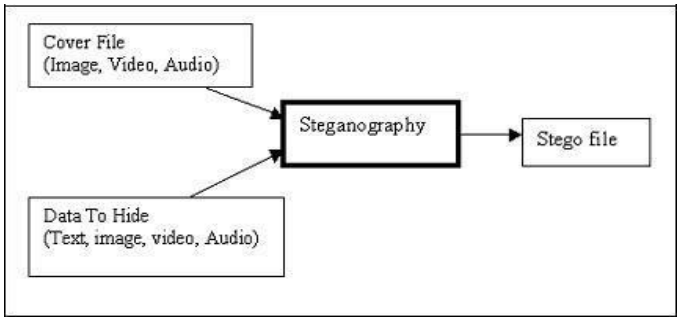


Figure 1: The Process of hiding data [3]

The means in steganography incorporate the written work the instant messages, encryption of the instant message is one of the choices accessible. Afterward, content is covered up in the chosen media and transmitted to beneficiary. At recipient end, turn around process is actualized to recoup the first instant message. Different methods utilized as a part of the craft of steganography is the game plans of different bits of the characters of the content in a picture or other media. Remembering the over, two records are required; the picture document and the content record that contains the information.
LSB influences the littlest changes of the 8 bits in this way it adjusts the picture to least [5]. The most well-known strategy utilized is called LSB (Least Significant Bit) Mechanism that is covering up if the information at all huge Bit (LSB) of the message.
Be that as it may, one of its real restrictions is little size of information which can be inserted in such kind of pictures utilizing just LSB. LSB is to a great degree powerless against assaults. LSB systems actualized to 24-bit designs are hard to identify in opposition to 8 bit arrange. Alternate systems incorporate Masking and Filtering. It is typically connected with JPEG. In this system picture information is stretched out by veiling mystery information over it. Accordingly, specialists do exclude this [7] as a type of Steganography.
All calculations utilized for an organization have advantages

and disadvantages and rely on the situations utilized. It additionally relies on the data to be inserted. Different methods created were thought about [9]. Section VI gives out the subtle elements of the proposed strategy.

## VI. Usage

Steganography, as characterized above is a system to shroud an information in a picture in such a way, to the point that it is unperceivable. To accomplish such result, one may consider cleaving the crude information that is the information to be covered up in break even with number of piece and shroud it in particular regions inside a picture. Such an idea translates, to the point that the idea isn't striking. That is, one can't remove the genuine excellence of Steganography. Directly the innovation being for the most part utilized is Digital Images By Computerized Images we dare to manage bits that is 0's and 1's.

Advanced Images we have chosen are 24-bit profundity shading pictures utilizing RGB shading model. 24-bit alludes to 8-bit for each RGB shading channel, i.e. 8-bits for red.8-bits for green and 8-bits for blue and 24-bit profundity with width and stature of 800 x 600 pixels. It must be recollected that picture determination is profoundly reliant on the screen determination.

The thought is to shroud message in picture with the conditions that the picture quality is held alongside the extent of the picture. Here, an idea may emerge that why we have to conceal message in a picture on the off chance that we can undoubtedly scramble is utilizing a few ways. This is where Cryptography and steganography varies. Applying, cryptography result in a yield of a unintelligible content (figure content), which when send over a web is effortlessly noticeable that some critical data is being passed on. Unexpectedly, concealing message in a picture, alongside the conditions, may appear to be only a trade of picture between two closures.

Now mind meanders that how a picture can contain a message with no adjustment in its quality and size. From this end onwards, we will give a short vision on the picture plan. Regardless, one must have a reasonable idea of an Image design which incorporates the Image Header data, Image piece data, Image extensible data (if any). Most of this data is unmistakably determined in standard specialized archives.

We are utilizing 24-bit BMP more than 24-bit JPEG in light of the fact that it is lossless pressure. JPEG is lossy i.e. to spare space on circle it just takes out parts of any picture. On the off chance that you look at the bit profundity and pixel estimation of a BMP and JPEG both have the same with the exception of the document measure on circle. The reason lies in the pressure conspire utilized by JPEG and BMP. In JPEG, pressure plot, Discrete Cosine Transformation (DCT) utilized, does not pack the information but rather sorts out it in an unexpected way, to such an extent that it decreases the span of the document by 50%. To make this pressure effective the shading model much be changed from RGB to YUV shading model. Presently the inquiry emerges, that why YUV show, reason lies in the way this shading model speaks to shading. Basically, RGB stores picture shading in blend however YUV isolates these shading in Y for Luminance (shading Brightness), U for chrominance (color contrast) and V for shading data. This approach is utilized because human eye is touchier to Luminance then chrominance. Thusly, less bits can be utilized for speaking to chrominance data. Lessening bits in chrominance is accomplished by applying chrominance down inspecting. In this manner, lessening the general size of an image. [8]

Our calculation is basic and adaptable utilizing LSB procedure. We have chosen the configurations that regularly utilize lossless pressure that is BMP, PNG, TIFF and GIF. We can make utilization of any of these configurations or change over BMP into any of the above said groups. At the point when information is gushed, it is caught after the header and slashed into 8 bits.

Figure 2: Simple conversion of a BMP to GIF

It has been investigated that the transformations don't contort the pictures to a level where the debasement can be felt with the exposed eye.

Figure 3: Simple conversion of a BMP to TIF

We prescribe this calculation to be utilized to shroud little measure of information albeit vast measure of information may likewise be consolidated in a picture. Information isn't embedded appropriate from the main byte caught however from an assigned area pre-settled on the two gatherings concerned. The idea is like to some degree one-time cushion. An extensive number of pictures from the said positions were concealed the information. Results affirm the utilization of these arrangements for fruitful Steganography methods. In 24- bit BMP, utilizing RGB shading model, with header size of 54 bytes.54 bytes onwards begin the pixel estimation of a picture. Every pixel esteem contains the estimation of the shading and is spoken to in bits (0 and 1). Similarly, content to cover up is additionally spoken to in bits (0&1).Therefore looking at bit esteems byte by byte bring about concealing the bit estimations of Text in bit estimation of an Image. The strategy we are utilizing is Least Significant Bit (LSB) i.e. putting away in LSB of a byte (pixel). As specified over, the

RGB show is utilized, we first stream an Image document and read the record in bits and after that look for the position ahead the header bits. In the wake of achieving the re-imagined area, read bits in gathering of 8 (byte) and supplant the last piece with the proposed information to be covered up in the picture.

Figure 4 Resultant image after hiding data in GIF format

Let us consider the above-mentioned images to hide the data. The topmost left area of image will compose of different shades of blue indicating sky and sea. Let us consider the first image pixel of value 194:213:243, 200:244:243, 192:213:243, (shade of a blue) of binary value 11000010:11010101:1110011:11001000:

Figure 5: Resultant image after hiding data in PNG format

11110100:11110011:11000000:11010101
and Text T of binary value 1010100.To store these 8 bits of character T, we will require 8 pixels. Since, we are using one bit of each pixel.
T = 1 0 1 0 1 0 0
Pixel Values 11000010:11010101:11110011:11001000:

In above sample consider the character T with binary values 1 0 1 0 1 0 0. Each bit is then replaced by LSB of each Image byte for e.g. First bit of T, 1 is compared with LSB of first Image pixel which is 1 1 0 0 0 0 1 0, zero. After reaching the redefined location, read bits in group of 8 (byte) and replace the last bit with the intended data to be hidden in the image.

Figure 6: A simple BMP Image

Since digital images are represented in bits and so is the text. The idea of playing with 0's and 1's seems quite simple but a slight change in value may transform an image completely, in other words distort an Image completely. Therefore, LSB is the most recommended bit to be used for hiding data.

Figure 6a: Above BMP Image after hiding data

## VII. CONCLUSIONS

Steganography is in the early phase of advancement. The proposed method cleaves the information in 8 bits after the header and utilizations LSB to conceal information from a pre- characterized position concurred between two gatherings. Same position is just utilized once to upgrade security. The significance of Steganography has not been acknowledged to that phase where it is favored over its nearby opponent "Encryption". New procedures are being found and executed. It is breaking down that time isn't far away when its significance would be acknowledged b associations by and large and the arm powers specifically. It is visualized that the same will happen soon as psychological militant exercises are on the expansion and it is suspected that work force in such exercises are trading maps and photos of potential focuses using Steganography.

## References

[1] D. Kahn, the Codebreakers, Macmillan, New York, 1967.
[2] Ahsan, K. &Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia,2002.
[3] Clair, Bryan. "Steganography: How to Send a Secret Message." 8 Nov. 2001 www.strangehorizons.com/2001/20011008/steganograph y.shtml
[4] Johnson, Neil F., and SushilJajodia. "Exploring Steganography:
Seeing the Unseen." IEEE Computer Feb. 1998: 26-34
[5] Denning, Dorothy E. Information Warfare and Security. Boston,
MA: ACM Press, 1999: 310-313
[6] KafaRabah. Steganography - The Art of Hiding Data. Information technology Journal 3 (3) - 2004
[7] Bret Dunbar. A detailed look at Steganographic techniques and their use in an open – systems environment: SANS Institute, 2002
[8] T. Moerland, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.Liacs.nl/home/tmoerl/priytech.pdf
[9] T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of

Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.

[10] Johnson, Neil F., and SushilJajodia, "Steganalysis of Images created using Current Steganographic Software", Proceedings of the Second Information Hiding Workshop, April 1998.

[11] Krenn, R., "Steganography and Steganalysis", http://www.Krenn.nl/univ/cry/steg/article.pdf