SMP LSB Steganography with Enhanced Cover Image: A New Multi-Level Security Approach with Visual Cryptography

Dr.Jithesh K[1*], Dr.Shameer A.P[2] , and Dr.Thomas Scaria[3]

1. Dept of Computer Science, M G College, Iritty,Kannur,Kerala.
2. Dept of Computer Science, NAM College,Kallikandy,Kannur,Kerala.
3. Dept of Computer Science, St.PiusXth College, Rajapuram,Kasargod,Kerala

---

Abstract:The main drawbacks associated with any existing steganography systems are, one, the distortion happens to the apparent view of the wrapper image after embedding and second the fewer hiding capacity of stego-image. When the confidential data is miniscule the system would be perfect. However, when the amount of secret data increases the disturbance caused is perceptible. Our aim with this proposed technique is to implement a stego system that gives maximum payload capacity with improved viscinity of the stego- image. With the slated objectives the proposed work try to maximize the security with high payload by enhancing the apparent view of the image so as to give no trace of hidden secret inside the cover.We propose a multi level security approach that uses visual cryptography for encryption to achieve security at first level and a brand new steganography method called Selected Matrices Pixels LSB [SMPLSB] at next level. In contrast to the distortion happens when hiding data inside a digital image, the projected technique enhances the host image quality while embedding. It finds a trivial location or less sensitive traits of the cover to embed the secret and make sure that embedding does not affect the original view of the image. The steps are repeated until the whole secret is hidden without disturbing the original view. Cover image preprocessing is also done to make the cover best suit for embedding.Our proposed approach cut short the chance ofsteg-analysis. It keeps a position map to assure the accurate fetching of hidden message. Higher PSN ratio of 50.1 dB, SSIM value of 1 and AAD 0.15050 show the projected method achieves good security with large payload .

Keywords: Steganography, visual cryptography,steganalysis, cover, SMPLSB

1. Introduction

The development of the current economic society was largely contributed by the shift of analogue data transfer to digital. Internet has also contributed a lot. The internet has become the conduit of all sort of communication and changed our day to day life in many ways. The modern paradigm of commerce called e-commerce allows persons to buy things through net. The digital world is revolving around the internet. As an open forum it has created some collateral issues. The information that has been shared through internet should be secure. The efficient, convenient and well-timed gaining of services through accessing the web still requires fine tuning for individuals and organizations. 5G has already been introduced worldwide but developing countries yet to wait for its out and out implementation. Meanwhile, astonishingly, countries like Japan declared their entry into 6G. In coming years the digital world is going to

[1]*Corresponding author: Jithesh K, email:jithukotheri@gmail.com*

witness a drastic change on data communication with high security. Nevertheless, the conveyance of critical information through an open conduit escalates the chances of potential threat. Several techniques have been proposed to deal with such type of issues. Steganography plays a vital role in information security for content authentication and perceptual transparency and no one can overrule its exigency.The main aim of information hiding is to conceal the secret data into the wrappers to avoid attracting the attention of possible attackers[1][2] in the Internet channel.

Steganography and cryptography are the two main techniques to provide information security. Kaur and Bansal (2014) [3] have mentioned that steganography is acquiring attraction by people due to security problems over internet. It is said that steganography and cryptography are the two sides of the same coin. However, what makes steganography more alluring is, steganography hides the very presence of the secret whereas the other reveals its presence. Since cryptography discloses the very existence of the secret, even if it gives high security and large payload the intruders are getting knowledge of the secret present and eventually they can try to hack the same with an expectation. This is the main issue of any powerful crypto system. Therefore no crypto system can claim total security. This makes steganography more attractive.

Embedding secret data (Steganography) has developed into a digital policy of file superimposing in some kind of multi-media such as digital image, a video or even an audio file. Lee and Chen (2000) [4]have described that the system of information hiding is described by having three varied perspectives that argue with one another namely robustness, security and storage capacity. Amount of data to be hidden is called capacity of a host medium. Security means thwarting of intruders from fetching the hidden data and robustness means the ability of the cover image to withstand before an adversary to destruct the hidden data.There is no need to explain the significance of digital communication at this new normal situation and it is conspicuous that in digital communication confidentiality is crucial when sensitive information is shared between entities over an insecured public channel.

The goal of steganography is to keep its existence not detectable. However, the steganography systemsalways leave behind detectable marks in the cover medium through changing its spatial as well as frequency traits. So attackers can predict the distortions in the resulting statistical properties of stego medium. The method of predicting these alterations is known as statistical steganalysis. Steganalysis[5] is a crucial topic that involves in detecting the presence of super imposed messages in stego-images. RS attack, put forth by Fridrich et al [6]in the year 2001, and x^2 detection, introduced by Westfield et al[7] in the year 1999 are the two most effective LSB steganalytic techniques. The former can identify both sequentially and randomly embedded messages and the later is good at detecting sequentially embeddedsecrets only. An extended version of Westfield et al has been proposed by Provos (2001) [8]to enhance its ability to recognize randomly hidden bits of the secret. Every one of the aforementioned techniques can precisely detect and estimate the length of the bits embedded in a host medium. While designing the projected algorithm we have taken care of these steganalysis.

All these strong detectors of can easily and precisely predict the presence of secret bits in digital images with greater accuracy. Therefore it is exigent to build a novel scheme of steganography that is strong enough to thwart attacks and suffice the capacity of payload. Storage capacity is not the key needs of a secret interaction. Developing the rate of embedding without compromising visual quality and security is the major concern for entire stenographers. Thus it can be inferred that the digital image steganography techniques depends mainly on robustness, imperceptibility, payload and embedding capacity to secure the information.

Only innovations that comprisesboth art and science can withstand the sophisticated way of eavesdropping at a certain extend. Though various spatial and frequency domain techniques have been carried out by many researchers, the development of large payload and highly secured stego-system with high peak signal to noise ratio still remains in texts. This study focused to develop stego systems that have large payload with high security. At this juncture any secured system with single level of security is easily breached. So, stego systems with multiple levels of security are the need of the hour. Multi level security means, mechanism where a message is encrypted or hidden more than once with different technologies. Few years back researchers are looking into systems that provide single level of security. The chances of security breaching in such cases were very high. Therefore people think of new methods that if implemented by combining different aspects of security mechanisms will give more security than the earlier one. Multi level security was first introduced by K Jithesh and A V S Kumar in the year 2010 [9] by blending steganography and cryptography to provide maximum security. Since then it emerged and became popular among the researchers of information security. The unlimited scope for research and additional scope for security prompted the authors to introducesuch a novel multi level security system that hides analready encrypted message inside a cover medium. Accomplishing this task authors combined a novel digital image steganography (Fabien Petitcolas A P., Stefan Katzenbeisser 2000)[10] scheme with popular visual cryptography (Naor M., Shamir A 1995) [11]. The scheme proposed here is an enhanced version of state of the art LSB method with large payload and imperceptible hiding technique.

As said, the proposed scheme combines features of both steganography and cryptography (William Stalling2019) [12]to overcome collateral issues and payload capacity. The purpose of this study is to introduce a technique to preserve security at one level even if the other level of security is breached.Human visual system is not so sensitive to digital images. Therefore digital images are deemed to be the awesome candidates for implementing steganography. Best among the spatial domain techniques is substitution technique, which hides secret bits by replacing original bits of the host medium. Redundant and noisy bits of digital covers are the best areas to hide secrets by replacing them with appropriate bits in the secret [13].It is easy to embed already encrypted secret inside a noisy cover without producing much distortion. After embedding, the image that acts as a host is referred to as stego-image. The key which is exigent for hiding or embedding is known as stego-key.

The advantage of this scheme is that since the secret is encrypted with cryptography before embedding the message will be safe evenif it is compromised at steganography

level and vice versa. In order to break the entire system, one has to find loopholes that are two times greater than the ordinary stego-system. To achieve this multi level security, we proposed the algorithm named selected matrix of pixels least significant bits [SMPLSB] replacement algorithm. This steganography method also concentrates to minimize the distortion or visual artifacts due to embedding. Security of a stego system is mainly associated with the visual quality of the stego image. Once the original view of the cover is disturbed or its innocuous nature is questioned, the very essence of the security is breached. Moreover we preprocessed the cover image to make it more suitable to hide large amount of secret without disturbing the original view. The experiments conducted proved that the introduced system is best in terms of assuring security.

The original quality of the stego-image, payload capacity and safety are the triple traits that have to be taken into account when creating a best steganography system. This study tried its best to keep up these problems by a technique that replaces LSBs of selected matrix of pixel values from the wrapper image.

2. Related Works

The LSB-replacement (Chan L.M. Cheng2004) [14], embedding method alters the LSB plane with secret message bits. There are other methods as well that do not replace bits when embedding. In LSB matching[15],it checks a match between the embedded bits with the LSB of the cover image and if found no match then the pixel value of the corresponding pixel is randomly added by ±1. LSB replacement and LSBMatching embed message bits pixel by pixel, whereas, LSBMR[15] handles the situation with two pixels at a time and permits minuscule changes to the image, which is opted for embedding the secret. The withstanding capacity against steganalysis and distortion to the original viewof the digital image of LSBMR are better than LSB Matching algorithm as well as Edge adaptive LSBMR (Lou W, Huang F, Huang J 2010) [16]. At large, the selection of locations for hiding inside a host image rely on a random series without considering the association amongst the content itself and the nature of the confidential data. Instead, LSBMR-EAintroduced later expands the LSBM Revisited algorithm and uses an edge-adaptive [16] mechanism to find the hiding locations to avoid pseudorandom selection. LSBMR-EA superimposes the secret bits of message from high intensity edge regions to low intensity edge regions, in accordance with the physical features of the message to be superimposed. Lou et al (2010) [16] confirmed that LSBMR-EA can boost up the safetyremarkably compared with the state of the art LSB-based approaches, while keeping better visual quality of the stego-images. Mansoor Fateh et al (2021) [17] proposed a scheme that points the pitfalls of LSBMR and recommends a new LSBMR scheme. The two phased scheme converts the covert data into a bit-stream, and later the bit-stream is partitioned into a set of chunks comprising n bits in eachand every chunk. Subsequently it chooses $2n - 1$ pixels for injecting such n bits of the covert data into the host image [Stego-image]. They claim that their scheme needs fewer changes than its previous version. However, though the embedding capacity is higher, it also shows higher detection error than most popular steganography methods of the time. The figure-1 illustrates the flow

chart of the popular LSB technique.

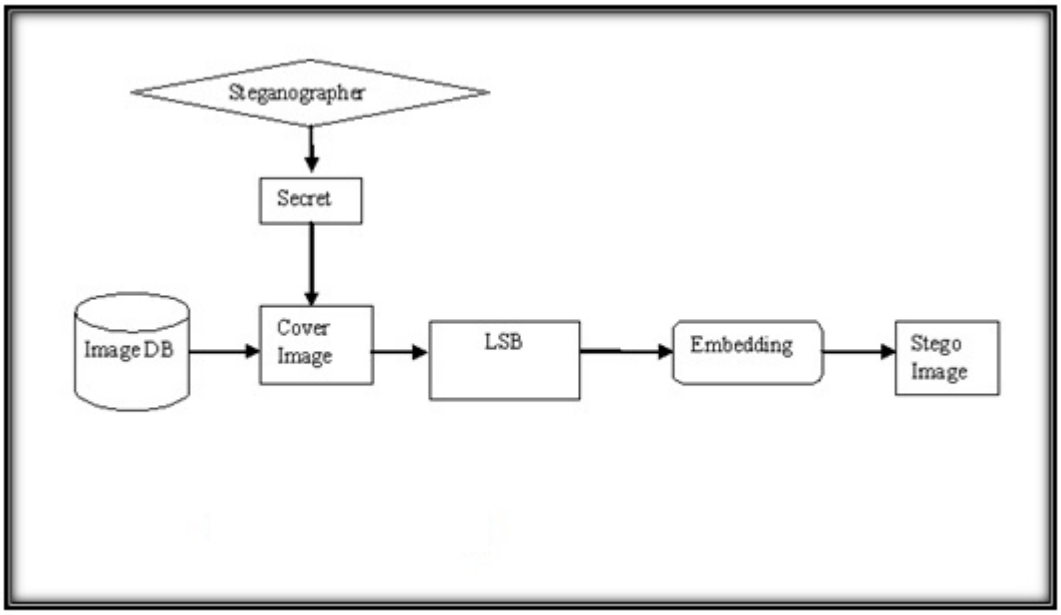


Figure 1. Flow chart of LSB

It is conspicuous that no technique is perfect and therefore lasts only for a very short period of time. So, without loss of generality, it can be asserted that no techniques mentioned above are able to achieve perfect stego-image quality andintricacy against attackers for a real life secret communication scenario where the amount of data is not fixed. The above methods are only good when the size of the secret is small. This made the authors of this proposed study to come out with a novel algorithm that gives high security and maximum payload capacity as far as a real time communication is concerned. Cover image distortion is the main issue associated with large payload. So when implementing this novel method authors are particular to give maximum security with large payload and cause no distortion to the original view of the cover. The quality of the images can sometimes be determined by taking into account of human vision sensitivity along with the help of available image processing techniques.

As said, no methods introduced either frequency domain or spatial or adaptive are not absolutely flawless. Out and out imperceptibility cannot be claimed by any known method and it's yet to be developed. This reality entice every researchers to develop a scheme that improves apparent vista of the digital image [cover] even after the secret is embedded. It is proved that peak signal to noise ratio cannot be infinite and hence no technique is completely free of distortions. Nevertheless, it is able to overcome the negative effect of embedding at a maximum extend.

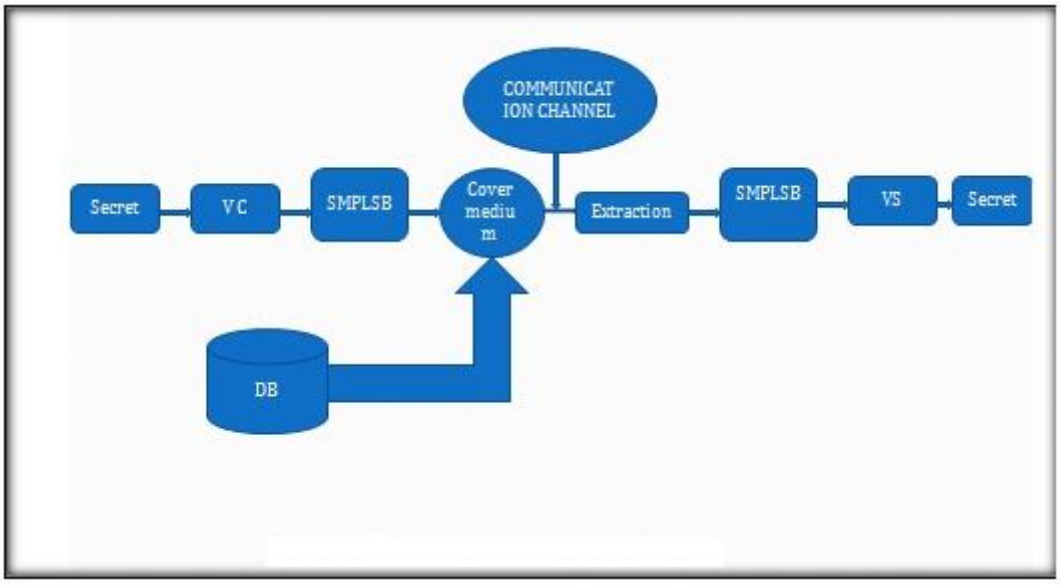
3. Proposed Multi-Level Security Approach

In this section the aforementioned scheme is explained in detail. The current trend in information hiding is to provide multi-level security by fusing two sides of information security. That is mixing cryptography and steganography (Shifa A, Asghar M. N, Fleury M, Kanwal N, Ansari M. S, Lee B, Qiao Y2020) [18]. Our proposed scheme that is SMPLSB combine's steganography with most prominent cryptography

method called visual cryptography [VC] (Patel D D, S Desai 2020) [19]. This technique replaces LSB of selected matrix of pixels of the cover image with secret. In thiscase the secret is in encrypted form. For encryption VC are used. The reason to encrypt the secret with cryptography before embedding is to provide multi-level security. It is unveiled with the intention to accomplish lofty imperceptibility and greater robustness to thwart hackers in contrast to the existing algorithms that provide single level of security.

This brand new technique has two stages; firstly, the confidential data is converted into shares using Visual Crypto System, put forth by Moni Naor and Adi Shamir(2006) [20]. The second step involves hiding these encrypted secrets into a digital image. The encryption and embedding involved in this two sided scheme is good enough to accomplish multi-level security. The output of one stage acts as the input of the next stage to enhance the security as well as the imperceptibility of the digital cover. Figure 2 shows the overall working process of the mentioned procedure.

In lieu of the common substitution technique; LSB, this study suggests to replace only selected bits of pixels from the cover image. Selection is done at random fashion. Each selection is compared with the original cover medium. If the substitution does not harm or enhances the image, that location is selected and the location point is stored. It is treated as stego-key. This key is secured with any of the message digest functions available and intimated to the receiver. The identified image must comprise noises and required number of intensity values and also it must seem very casual.



Fig,2-Flow chart of the proposed method

3.1Encryption with visual cryptography- First Level Hiding

At the outset the secret data is first converted into visual shares using (2, 2) visual cryptography. Here the secrets we concentrated are only visual texts rather than images. Using advanced VC algorithm the security can be improved. This is the initial level of the proposed technique. The obtained share1 and share 2 of the information is

embedded inside the cover Image. The cover image should be of a dimension greater than or equal to 512 X 512. Image shares of the secret will be converted into its binary form before embedding. So the intensity value of the pixels of the secret to be embedded would be only one bit either zero or one. Therefore the embedding process through substitution is very easy and it will not cause any significant distortion to the apparentvisible nature of the host (cover) image. In the hiding stage, subsets of cover-elements from the host image are selected as candidates for performing replacement operations to embed bits of confidential data. That mechanism is described in the following section.

3.2 Proposed Selected Matrix of Pixel's LSB [SMPLSB]

At the outset a matrix of order n x m is selected from the entire pixel values of a cover image. The selection of a required matrix of pixels of the cover is done by considering human visual system and statistical analysis using image processing tools. This will help to find out the most suitable or in other words, insignificant regions of the cover image to hide the secret. The value of n and m of the selected matrix are determined from finding the size of the VC shares of the secret that are going to be embedded. As mentioned the VC shares of the secret text image are converted in to their binary form before embedding. The binary representation of any image consists of only 1s and 0s (ones and zeros) as their pixel values. That is only one bit is required to represent each pixel. Therefore,if the cover image is a grayscale, hiding each one of these one bit pixel requires only one bit among the eight bits of each picture element (pixels) of the cover image. The cover image could be either gayscale or colour. Here the secret is the text '***hello'***. Its VC shares are illustrated in fig.3. The fig.4 shows the binary pixel values of the VC share 1. As per the SMPLSB we need to take out a matrix of the order 5 X 16 from the picture element (pixel) values of the cover image. Figure-5 of Gandhi picture is selected as the cover image and figure-6shows the selected matrix of pixel values of the Gandhi image for hiding the secret bits shown in figure-4. Since the secret share consists of 5 X 16 values the cover matrix should also be of the same size. With SMPLSB algorithm discussed in section 3.3.1, it is able to hide the secret inside the selected matrix. A case in point is also seen in figure-6.

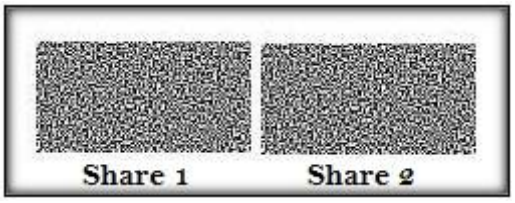


Figure 3: Visual cryptography case in point

0	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1
1	0	1	1	1	1	1	1	1	0	1	0	1	1	1	1
1	0	0	0	1	0	0	0	1	0	1	0	1	0	0	0
1	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0
0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0

Figure 4: Binary pixel values of the VC share 1

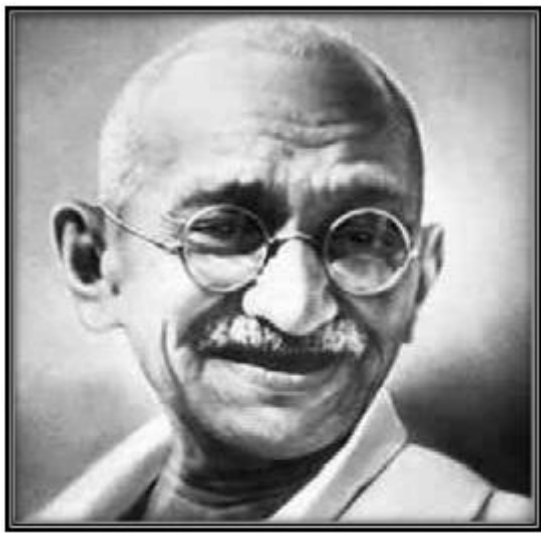


Figure 5: The cover image

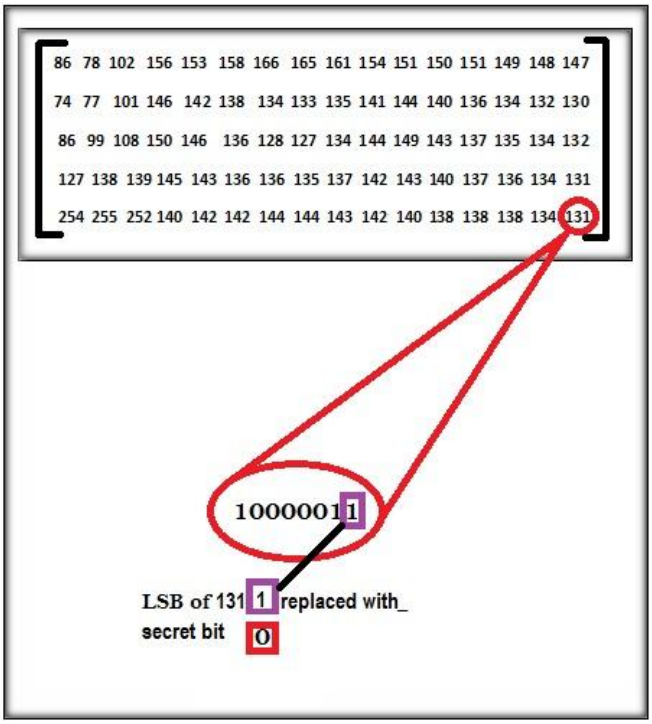


Figure:6 Embedding procedure

3.2.1Steps of Encoding Process of SMPLSB

1. Choose the secret to be encrypted, say Mi.
2. Using VC divide the content of the message (Mi) into shares. [first level security]
3. Each of the share is a secret to be embedded.
4. Convert these shares into binary format
5. Find out the number of binary bits present in the shares. It is of the form of an [n X m] matrix.
6. Select an appropriate cover image to embed the secret shares. It is possible to have more than one cover. However, using more covers to hide a single secret may cause larger overheads.
7. Select two appropriate matrices of pixel values (intensity) of order n X m from the cover which is sufficient to hide the secret.
8. Replace each LSB of the selected matrix of intensity values with the cryptic bits.
9. The four coordinate points of the selected matrices of pixel values will act as the stego key.
10. Stego key can be send with public key crypto system.

3.2.2 Steps of Decoding Process:

1. Decrypt the stego-key.
2. It gives the location map of the matrix of intensity values where secret shares are embedded.
3. Take out each LSB of the matrices. The bits extracted in this way out of the selected pixels of the stego-image are in the form of binary. Each such obtained binary represents visual share of the secret.
4. These shares can then be superimposed one on another by means of a computer and extract the original message. It requires no computation.
5. Or rather print outs of the shares can be collected and super imposed to form the original secret.

4. Results and Discussions

To evaluate the performance of SMPLSB method we conducted many experiments.The algorithm starts with the prominent visual cryptography. It slices the original message into two (2) shares. Visual cryptography plays a very good role in information security. The popularity of VC system relies in its capacity to decrypt the secret from its shares without any sort of computational operations. These secret shares such obtained will be injected (hidden) into the cover image using the brand new SMPLSB steganography algorithm. Experiments have been done with different images. One among is shown in Fig.3 to Fig.6. Here encryption by visual cryptography gives one level of security. At the next level these shares are rooted into a digital cover with SMPLSB steganography. Here the second level of security is also obtained.

From the experiments conducted with different wrappers and secrets, it is proven that this proposed technique is one among the best of available spatial domain techniques. The real advantage of this technique is that, since the VC shares are in the form of binary,each single bit represents anentire pixel. Hence it is possible to hide each pixel value by substituting (replacing) only one bit of the cover image. Another advantage of this technique is that, because the secrets are in either 1 or zero, in most cases the cover image LSB may be same as that of the bit of the secret and hence it is not required to be altered. The PSNR value of the original digital image and the stego-image show that the distortion happened to the apparent view of the former is imperceptible. Considering all these facts this technique can easily claim that the issues of distortion and perceptibility pertaining to steganography are reduced at a possible minimum level and as stated earlier, it improved the security by blending with visual cryptography. We have conducted a comparative study of our scheme with unsophisticated LSB based schemes like LSB, BPCS [21]and AE-depth varying scheme (He J., Tang S., Wu T 2008) [22] and found that our scheme has better PSNR, SSIM and AAD values than others. We also done a comparative study of our scheme with currently popular methods like Multiple LSB Substitution and Pixel Randomization Using Stern-Brocot Sequence[23], a scheme introduced by Dalia N and Loay M(2019), entitled 'An efficient steganographic technique for hiding data'[24] and a new AE method proposed by K Tiwari and Sahil J (2020) [25].The high PSNR of our scheme, obtained from both the experiments done on old andnew methods,prove our scheme have better security as well as high competent quality to the cover image. The results are flaunted in table-1and table-2 as follows.

Table.1 PSNR, SSIM & AAD of stego-images obtained from different steganography schems.

Methods	PSNR	SSIM	AAD
LSB	45.4	0.9999	0.29941
BPCS	45.8	0.9999	0.29878
AE-Depth	49	1	0.15075
Our scheme	50.9	1	0.15050

Table.2 PSNR, SSIM & AAD of stego-images obtained from current popular steganography methods.

Methods	PSNR	SSIM	AAD
Dalia N and LoayM[39]	34.8	0.8	0.26941
Md. Abdullah A M et al[38]	45.8	0.8	0.28878
K Tiwari and	48	1	0.15045

Sahil J [40]			
Our scheme	50.9	1	0.15050

5. Conclusion

The selected matrix of pixel's least significant bit [SMPLSB] hides VC shares of the secret inside a visually insignificant region of cover image. Since this method converts the shares into their corresponding binary, one bit is enough to represent the secret. So it can save many spaces inside the cover and consequently it can store more data than a conventional stego system. This method is best suited to embed text messages where contents are important rather than its vicinity. But text messages should be converted into its VC shares before hiding. Therefore we blended visual cryptography with this projected steganography. The advantage of this method is since replacement needed to the LSB of the selected pixels are very less the visual disturbance caused due to steganography with this technique is little noticeable. Apart from this the improvement in multi level security due to the blend with visual cryptography is highly recommendable. Another important aspect of this technique is; it does require less computation than other two studies of this chapter. Nevertheless the payload of this tech is comparatively less.

References

1. Frank Y., Shih (2008), Digital Watermarking and Steganography Fundamentals and Techniques. CRC Press, Taylor & Francis Group.
2. Forouzan B A, Mukhopadhyay D, Cryptography and Network Security-Principles and Practices, Mc Graw Hill, 3rd edition, (2017).
3. Kaur N and Bansal A (2014), A review on Digital Image Steganography, International Journal of Computer Science and Information Technologies, Volume 5 (6), pp 8135-8137.
4. Lee K. and Chen H (2000), "A High Capacity Image Steganographic Model," in IEEE Proceedings on Vision Image and Signal Processing, China, pp. 288-294.
5. Wu Z,Guo J, Zhang C, Li C (2021), Steganography and Steganalysis in Voice over IP: A Review. Sensors 1032.
6. Fridrich J., Goljan M., Du R.(2001), "Reliable detection of LSB steganography in color and grayscale images", in Proceedings of ACM Workshop Multimedia and Security, pp. 27–30.
7. Westfeld A., Pfitzmann A.(1999), "Attacks on steganographic systems", in Proceedings of the 3rd International Workshop on Information Hiding, Dresden, Germany, pp. 61–76.
8. Provos N.(2001), "Defending against statistical steganalysis", in Proceedings of the 10th USENIX Security Symposium, Washington, DC, p. 24.
9. K Jithesh, A V S Kumar,(2010),"Multi layer information hiding -a blend of steganography and visual cryptography", Journal of Theoretical and Applied

Information Technology 19(2), pp.109-116.

10. Fabien Petitcolas A P., Stefan Katzenbeisser,(2000), Information Hiding Techniques for Steganography and Digital Watermarking, artech house, inc. 685 Canton Street Norwood.
11. Naor M., Shamir A.(1995), "Visual Cryptography, Advances in Cryptology", in Proceeding Eurocrypt,94 , LNCS vol. 950, Springer-Verlag, 1-12.
12. William Stalling, (2019), Cryptography and Network Security-Principles and Practices, fourth edition.
13. Rengarajan A, John Bosco BalaguruRayappan, (2012), "An intelligent chaotic embedding approach to enhance stego-image quality", Information Sciences, 193, pp.115–124.
14. Chan, L.M. Cheng,(2004), "Hiding data in images by simple LSB substitution", Pattern Recognition 37 (3), pp.469–474.
15. J. Mielikainen, (2006), LSB matching revisited, IEEE Signal Processing Letters,Volume: 13 , Issue: 5 , pp.285-287.
16. Lou W., Huang F., Huang J. (2010), "Edge adaptive image steganography based on LSB matching revisited", IEEE Transactions on Information Forensics and Security . Security 5 (2), pp.201–214.
17. Mansoor Fateh , Mohsen Rezvani, Yasser Irani,(2021) "A New Method of Coding for Steganography Method on LSB Matching Revisited", Security and Communication Networks, Vol.
18. Patel DipakkumarDhansukhbhai, Dr. Subhashchandra Desai,(2020), A New Approach for Multilevel Steganography Using Visual Cryptography for Multimedia Application". International Journal of Advanced Science and Technology, 29(2), pp.4667 - 4684.
19. Shifa A., Asghar M. N., Fleury M., Kanwal N., Ansari M. S., Lee B., Qiao Y.,(2020), MuLViS: Multi-Level Encryption Based Security System for Surveillance Videos. IEEE Access, 8, 177131–177155.
20. Naor M., Shamir A.,(2006), "Visual Cryptography II: Improving the Contrast Via the Cover Base", Security in Communication Networks , pp.197-202.
21. Cong-Nguyen BUI, Hae-Yeoun Lee, Jeong-Chun JOO, Heung-Kyu LEE,(2010), "Secure bit-plane based steganography for secret communication", IEICE Transactions on Information and Systems, vol.E93-D No.1, pp.79-86.
22. He J., Tang S., Wu T,(2008), "An adaptive image steganography based on depth-varying embedding", Image and Signal Processsing, vol. 5, pp.660–663.
23. Md. Abdullah Al Mamun et al,(2020),A Novel Image Steganography Using Multiple LSB Substitution and Pixel Randomization Using Stern-Brocot Sequence, Advances in Information and Communication, pp.756-773.
24. Dalia Nashat, Loay Mamdouh, An efficient steganographic technique for hiding data, Journal of the Egyptian Mathematical Society volume 27, Article number: 57, (2019).
25. Tiwari K, Sahil J. Gangurde,(2020), LSB Steganography Using Pixel Locator Sequence with AE.

26. Singamaneni, Kranthi Kumar, Pasala Sanyasi Naidu, and Pasupuleti Venkata Siva Kumar. "Efficient quantum cryptography technique for key distribution." Journal Europeen des Systemes Automatises 51.4-6 (2018): 283.
27. Singamaneni, Kranthi, Abdullah Shawan Alotaibi, and Purnendu Shekhar Pandey. "The Performance Analysis and Security Aspects of Manet." ECS Transactions 107.1 (2022): 10945.
28. S. Kranthi Kumar, A. Alolo Abdul-Rasheed Akeji, T. Mithun, M. Ambika, L. Jabasheela et al., "Stock price prediction using optimal network based twitter sentiment analysis," Intelligent Automation & Soft Computing, vol. 33, no.2, pp. 1217–1227, 2022.
29. Rekha Baghel, D.Saravanan, et.al., "Reclamation of extraordinary utility items in the multi-level catalogue", Recent Trends in Science and Engineering, AIP Conf. Proc. 2393, 020195-1–020195-11; https://doi.org/10.1063/5.0074502, Published by AIP Publishing. 978-0-7354-4198-9/$30.00.
30. D.Saravanan, et.al., "Optimization of Machine Learning and Deep Learning Algorithms for Diagnosis of Cancer", ECS Transactions, Volume 107, Number 1, DOI: https://doi.org/10.1149/10701.9389ecst.
31. D.Saravanan, et.al., "Customer Relationship Management in Banking in the UK Industry: Case of Lloyds Bank", ECS Transactions, Volume 107, Number 1, DOI: https://doi.org/10.1149/10701.14325ecst.
32. D.Saravanan, et.al., "Brand Influencing Customers Buying Behaviors: A Case Study on Nike", ECS Transactions, Volume 107, Number 1, DOI: https://doi.org/10.1149/10701.5597ecst.
33. D.Saravanan, et.al., "Simulation of Carbon Nanotubes and NANO Based Material for Molecular Device Applications", ECS Transactions, Volume 107, Number 1, DOI: https://doi.org/10.1149/10701.13403ecst.
34. D.Saravanan, et.al., "Customer Relationship Management in Banking in the UK Industry: Case of Lloyds Bank", ECS Transactions, Volume 107, Number 1, DOI: https://doi.org/10.1149/10701.14325ecst.
35. D Saravanan, K Santhosh Kumar, "IoT based improved air quality index prediction using hybrid FA-ANN-ARMA model", Elsevier Materials Today Proceedings.
36. DL Shanthi, K Arumugam, D. Saravanan, et.al., "Optimized artificial neural network assisted trade-off between transmission and delay in LTE networks", Elsevier Materials Today Proceedings.
37. M Chandragowda, D Saravanan, et.al., "Consequence of silane combination representative on the mechanical possessions of sugarcane bagasse and polypropylene amalgams", Elsevier Materials Today Proceedings.
38. A Srinivasa Rao, D Saravanan, et.al., "Supervision calamity of public opinion actions based on field programmable gate array and machine learning", International Journal of Nonlinear Analysis and Applications, Volume No:12, Issue No:2, July 2021.
39. R. Abish, D. Stalin David, "Detecting Packet Drop Attacks in Wireless Sensor Networks using Bloom Filter", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 730-735, March-April 2017.
40. A. Vignesh, D. Stalin David, "Novel based Intelligent Parking System", International Journal of Scientific Research in Computer Science, Engineering

and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 724-729, March-April 2017.

41. D Stalin David, 2020, 'Diagnosis of Alzheimer's Disease Using Principal Component Analysis and Support Vector Machine, International Journal of Pharmaceutical Research, Volume 12, Issue 2, PP.713-724.
42. Jaswanth K S, Dr. D. Stalin David, "A Novel Based 3d Facial Expression Detection Using Recurrent Neural Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 48-53, March-April 2020.
43. D Stalin David, 2020, 'An Intellectual Individual Performance Abnormality Discovery System in Civic Surroundings' International Journal of Innovative Technology and Exploring Engineering, Volume 9, Issue 5, PP.2196-2206.
44. D Stalin David, 2020, 'Machine learning for the prelude diagnosis of dementia', International Journal of Pharmaceutical Research, Volume 13, Issue 3, PP.2329-2335.
45. David, D.S. and Y. Justin, 2020. A Comprehensive Review on Partition of the Blood Vessel and Optic Disc in Retinal Images. Artech J. Eff. Res. Eng. Technol., 1: 110-117.
46. Stalin David D, Saravanan M, "Enhanced Glaucoma Detection Using Ensemble based CNN and Spatially Based Ellipse Fitting Curve Model", Solid State Technology, Volume 63, Issue 6, PP.3581-3598.
47. Stalin David D, Saravanan M, Jayachandran A, "Deep Convolutional Neural Network based Early Diagnosis of multi class brain tumour classification", Solid State Technology, Volume 63, Issue 6, PP.3599-3623.
48. Dr. D. Stalin David, Mr. D. Saravanan, "Certain Investigation On Iot Therapeutic Image Recognition And Rivaroxabanpreclude Thrombosis In Patients", 2021, pg.no:51-66, ISBN: 978-81-948555-1-4.
49. R.Parthiban, Dr.K.Santhosh Kumar, Dr.R.Sathya, D.Saravanan," A Secure Data Transmission And Effective Heart Disease Monitoring Scheme Using Mecc And Dlmnn In The Cloud With The Help Of Iot", International Journal of Grid and Distributed Computing, ISSN: 2005 – 4262, Vol. 13, No. 2, (2020), pp. 834 – 856.
50. R.Bhavya, G.I.Archanaa, D.Karthika, D.Saravanan," Reflex Recognition of Tb Via Shade Duplicate Separation Built on Geometric Routine", International Journal of Pure and Applied Mathematics 119 (14), 831-836.
51. D Saravanan, R Bhavya, GI Archanaa, D Karthika, R Subban," Research on Detection of Mycobacterium Tuberculosis from Microscopic Sputum Smear Images Using Image Segmentation", 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).
52. D Saravanan, R Parthiban," Automatic Detection of Tuberculosis Using Color Image Segmentation and Statistical Methods", International Journal of Advance Research in Science and Engineering, Volume 6, Issue 10.
53. U.Palani, D.Saravanan, R.Parthiban, S.Usharani," Lossy Node Elimination Based on Link Stability Algorithm in Wireless Sensor Network", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue 6S5.
54. S.G.Sandhya, D.Saravanan, U.Palani, S.Usharani," Handover Priority to the Data at Knob Level in Vanet", International Journal of Recent Technology and

Engineering (IJRTE), Volume 7, Issue 6S5.

55. D.Saravanan R.Parthiban, U.Palani S.G.Sandhya," Sheltered and Efficent Statistics Discrimnation for Cluster Based Wireless Antenna Networks", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue 6S5.
56. Raghu Raman D, Saravanan D, Nivedha R," An Efficacious E-Portal for Rancher to Buy Seeds and Humus", International Journal of Recent Technology and Engineering (IJRTE), Volume-8, Issue-1S5, June 2019.