DOI : https://doi.org/10.56452/7-792

ISSN: 0974-5823 Vol. 7 No. 1 January, 2022

International Journal of Mechanical Engineering

Image Enhancement Using Histogram Shifting Technique for Reversible Data Hiding

Sushant Chamoli

Asst. Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Abstract

Digital image processing is the process of enhancing the clarity and quality of a picture. Also, owing to the requirement for security while emailing the recipient a picture. Reversible data hiding (RDH) is a key component of many current systems used to encrypt and decrypt pictures, allowing for easy improvement of the original image's quality without pixel loss once it has been embedded. Previous methods for embedding data into encrypted images by reversibly releasing space from them may have had drawbacks for data extraction and image restoration. Hence, by reducing data loss, this technique enhances picture security while also improving image quality at the receiver end. The rapid spread of information and the development of digital technologies, which have made it possible for information to be concealed in multimedia data, have made it easier to access digital data and made it possible for it to be stored, transferred, and processed in a reliable, quick, and efficient manner. This has had the unintended consequence of making it simple and covert to produce and distribute digital media illegally.

1. INTRODUCTION

The construction of cryptographic primitives with chaotic behaviour and random-like features has frequently employed dynamical chaotic systems in recent years. Shannon noted the outstanding applications of dynamical chaotic maps in communications in his pioneering work. He determined that dispersal and confusion are the two fundamental characteristics that successful data encryption systems ought to possess in order to thwart (resist) statistical assaults. The original data and the encrypted data may not be related to one another due to misunderstanding, which may also spread a change over the whole encrypted data set. The simplest kind of diffusion is permutation, which rearranges items, while the simplest form of confusion is substitution, which swaps out one object for another. The fundamentals of deep cryptography consistently make use of permutation and substitution techniques based on dynamical chaotic systems.

Data hiding refers to a range of methods used to embed secure data in host media (such as photos) with little host degradation and the ability to retrieve the secure data afterwards. You may mention steganography as an example. One such security-friendly invention is steganography, which embeds confidential information in a cover. Reversible data-hidings allow for the precise (lossless) restoration of the original host signal after the embedded information has been extracted. They do this by altering the host signal to add information bits. Reversible watermarking is occasionally used interchangeably with terms like distortion-free, invertible, lossless, or erasable watermarking.

The little distortion brought on by data embedding is often tolerated in the majority of applications. Yet, several industries, including legal, medical, and military imaging, consider the ability to reconstruct the exact original picture to be a desired quality. Let's imagine that private papers (such as bank checks) are scanned, secured using an authentication system based on reversible data concealing, and transmitted over the Internet. Most of the time, the watermarked documents will be enough to clearly identify the contents of the documents. In the event that any doubt develops, it would be quite intriguing to obtain the original, unmarked document.

A spread spectrum signal matching to the information payload is overlaid on the host during the embedding phase of Type I algorithms that use additive spread spectrum, and Type II algorithms that use modulo arithmetic, where information bits are embedded by changing, for example, overwriting, chosen aspects of the host signal. When using Type II algorithms, the original host signal is recovered by exchanging the modified features with the uncompressed original features at the decoder. This is done by compressing the original features and delivering the compressed bit-stream as part of the embedded payload.

Steganography is the technique of concealing data by concealing the message's very existence, making it impossible for a viewer to determine whether a message is being transmitted and, thus, impossible for them to attempt to decipher it. Steganos, which means "covered, concealed," and graphein, which means "writing," are combined to make this term, which is used in information security. The art of steganography involves concealing sensitive information under cover pictures to create stego images.

It is a recently created information security approach that has drawn considerable interest from both business and academia. Digital watermarking and steganography with encryption are the two primary disciplines involved. Steganography may use text, images, audio, and video as its carrier. The ability to conceal information in picture, video, audio, or text files with steganography software is improving. Steganography's fundamental goal is to securely communicate while concealing the real message from the observer. Using the Haar integer wavelet transform and controlled contrast enhancement (CCE), this system presented a novel RDH technique (IWT).

2. LITERATURE SURVEY

In this research, video steganography using digital watermarking methods is presented as a reliable and effective security solution. Together with certain standard operating procedures and recommendations culled from the literature, it offers an overview and critique of the various steganographic and watermarking techniques now in use. Text messages are concealed using DWTs, and the fundamental spread spectrum (SS) approach tries to disseminate hidden information throughout the frequency spectrum of an audio transmission using a code that is unrelated to the signal itself. Direct sequence and frequency hopping Spread Spectrum schemes are two types of Spread Spectrum that can be utilised in steganography. This article examined several embedding and security strategies. It was discovered that the spatial domain and least significant bit (LSB) techniques are the most effective methods for obscuring a hidden message or picture in cover material. DWT and DCT, which both have excellent resilience and are often employed in digital picture watermarking, are the best transform domain approaches for securing the hidden message. By breaking down a time domain signal into its frequency components, DCT produces a variety of frequency coefficients, including low frequency coefficients, mid frequency coefficients, and high frequency coefficients [1].

In order to find hidden information buried in digital photographs, this research suggests a general method for steganalysis. It employs feature selection techniques like ANOVA to choose pertinent characteristics, wavelet-like decomposition to develop a higher order statistical model of realistic pictures, and linear SVM algorithms to distinguish between clean and stego images. Contrary to arbitrarily complex non-linear classification methods like the neural network, the nonlinear classification is accomplished by first embedding training data into a higher (potentially infinite) dimensions space and then mapping it back to the original data space as a linear classification surface. There may be a false alert since JPEG-based steganographic embedding techniques (outguess) recompress the JPEG picture before embedding the message in it. Performance of the steganalyzer is impacted by the JPEG picture quality factor. High quality characteristics make it harder to discern between cover and stego photos, which might reduce the effectiveness of detection. ANOVA is used to examine whether statistics are consistent and reliable against the impacts of different steganography techniques, which helps to minimise complexity and boost detection accuracy. An all-encompassing method of steganalysis is presented that can identify the embedding algorithm regardless of the cover image type, compression ratio, embedding capacity, or embedding technique employed. It depends on creating a statistical model using statistics of the first and higher orders that are taken from multiscale, multiorientation picture decompositions. It is demonstrated that while these statistics are generally stable across a wide variety of pictures, the existence of concealed signals causes them to become unreliable [2].

The halftoning procedure, however, lowers the picture quality, and as visual cryptography systems also lower image quality, limiting image degradation becomes a key goal. This study uses an intelligent halftone picture

pre-processing based on the properties of the original secret image to investigate extended visual cryptography without expansion. A certain amount of black and white pixels are used as the foundation for the block replacement procedure in the SBR pre-processing approach. This image is now prepared to be utilised as a secret image in visual cryptography methods like classic VC or EVC and is known as a processed secret image. The pre-processing strategy may be used for other applications as well, such multiple image visual cryptography, which conceals many pictures in sharing [3].

Steganography is the technique of hiding information to transfer it so that only the intended recipient is aware of its presence. Viewing the statistical characteristics of the picture or medium in which the message is buried is one of the ways to find the hidden message using steganalysis techniques, which aim to dispel doubt about the presence of a message. This essay describes the nature of such assaults and offers conclusions based on analyses of the current countermeasures. The Discrete Cosine Transform (DCT) is used in JPEG pictures to accomplish image compression. Information is concealed in the JPEG image by changing the rounding decisions made for the DCT coefficients, either up or down. The current situation in the extremely stimulating subject of steganalysis, which has a lot of promise for further study, has been documented and described in this work. The methods employed in the status quo are sufficiently complex and can offer enough defence against present attacks, but with the increased public awareness of steganography and the plethora of transmission medium for pictures and concealed information, it is only foreseeable that attack tactics will only get more sophisticated. We must continuously look out for new attack vectors and develop defence strategies to counter them [4].

Steganography is the practise of writing that is concealed or covered in order to keep a message secret from a third party. This system's goal is to use Steganography to create security while using an image as the data carrier. The picture will open in any image previewer but won't show the contents if it is compromised or interpreted by a third party user since the data file is encrypted and authenticated. As the old system's technique was complex, it was challenging for the enclosure to distinguish between the data and the picture file. The major goal of this system is to conceal a significant quantity of encrypted and verified data, regardless of the image's size, dimensions, and clarity. This system's major goal is to conceal substantial volumes of encrypted and verified data while maintaining the image's sharpness. In order to embed the data before it can be transferred, this approach entails identifying the cypher text with the key (encr2) and the picture. Finding the size of the original picture requires opening the image in binary mode. The data from the picture is retrieved using a unique signature. It cannot be added if the image already has some info in it [5].

3. PROPOSED SYSTEM

The usage of symmetric encryption methods like Data Encryption Standard (DES) and Picture Steganography is covered in this study. DES was applied using the MATLAB programme, and the Avalanche effect parameter served as the basis for analysis. Steganography is the practise of concealing images in other pictures or films so that they may be sent securely. The system suggested using the location map to mark the highest and lowest spots in the histogram of the original image, although this would somewhat restrict the system's capability. Transforming the cover picture into a new domain is the initial stage in transform domain techniques, after which the altered coefficients are processed to obscure the secret data. Although transform domain approaches have a strong capacity to handle signal processing tasks, they are ineffective because of their low data embedding rate and poor visual quality.

DOI : https://doi.org/10.56452/7-792

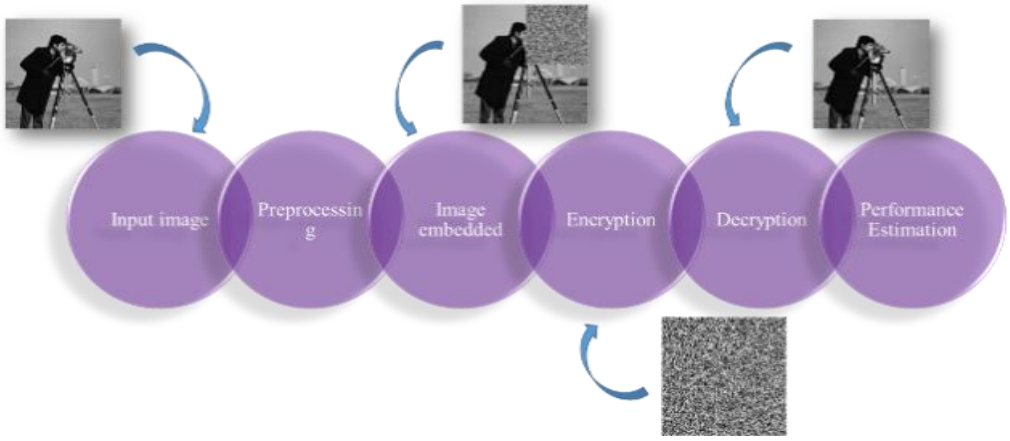

Fig 1: System Architecture

By employing a public key cryptosystem and the RDH and LSB algorithms to reserve space prior to encryption, the suggested technique makes it incredibly easy for the user to embed data in the encrypted picture. This allows for data extraction and picture recovery without any data loss because the image is reversible (pixel). The RDH and LSB algorithms have been mined because they can recover the original picture from a marked image without causing any data loss. With the same level of image quality and restoration, this RDH approach may be incorporated in more than 10 times as large of a content. The modifications in the coefficients for the horizontal, diagonal, and vertical subbands have relatively little impact on the contrast of the image. Using the companding approach, more message bits are inserted into the detail subbands. The length of the location map, the companding error, the threshold, and the compressed location map, as side information, should be included into the cover picture together with the message bits for the restoration of the original coefficient. The following are some of the proposed approach's benefits:

- That works quite well.
- It is capable of flawlessly restoring the original cover picture.
- The embedded bits can be extracted by it.
- The rate of data embedding is high.
- High visual quality.

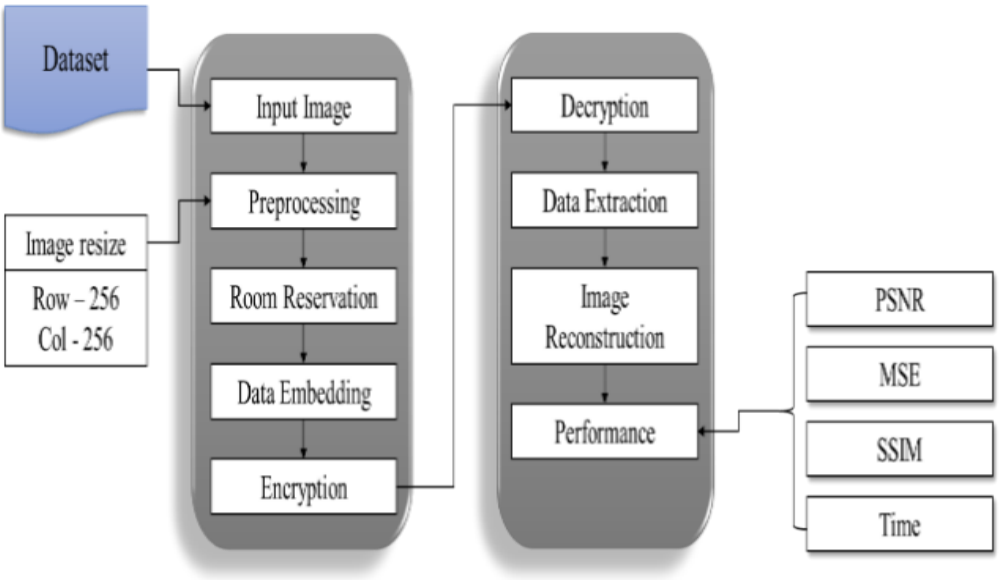

Fig 2: Flow Diagram

DOI : https://doi.org/10.56452/7-792

4. RESULTS

Reversible data hiding (RDH) is a technique used in digital image processing to increase both the security and quality of the picture during the receiver side. This is a result of the quick spread of digital technology and the simplicity of access to digital data. The primary goals of this method are to transport data securely and prevent data loss during picture encryption and decryption. The least significant bit and reversible data concealing are coupled to embed and retrieve the data in this suggested approach, which enables 100% data loss to be restored at the moment of data extraction. Public key cryptography is used to encrypt images, lowering the possibility of a data breach and enhancing data security.

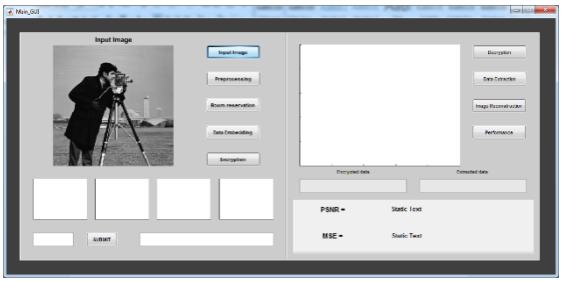

Fig 3: Input Image

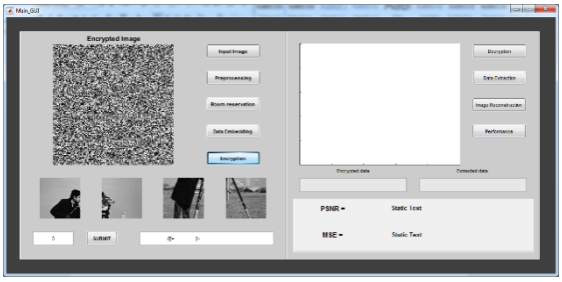

Fig 4: Encryption

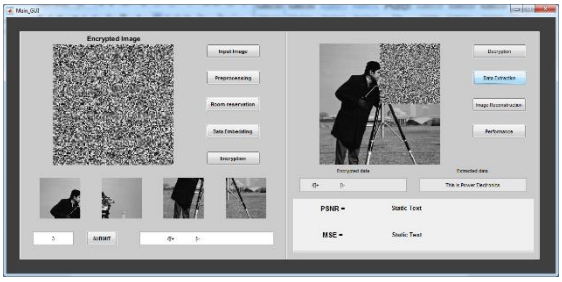

Fig 5: Data Extraction

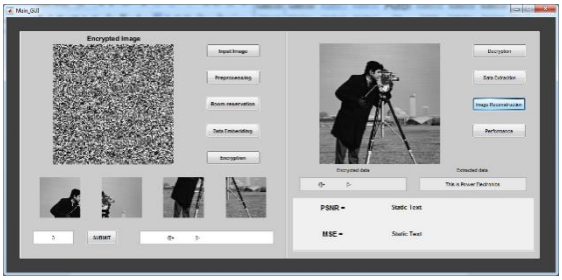

Fig 6: Image Reconstruction

DOI : https://doi.org/10.56452/7-792

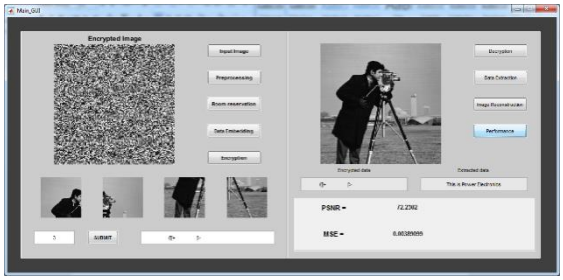

Fig 7: Performance Analysis

5. CONCLUSION

Whole loss of data can be restored as much as feasible at the time of data extraction by applying the suggested approaches. This suggests combining the least significant bit, reversible data concealment, and least amount of lossless data to embed and retrieve the data. Public key cryptography is used to encrypt images. We can draw the conclusion that data security has greatly expanded while data attack prevention has decreased. Data will be sent in secret and with a high level of security.

6. FUTURE SCOPE

Picture encryption is a crucial and practical method for safeguarding image security. Future research will offer a revolutionary picture encryption technique that combines Julia sets and Hilbert curves. The approach uses the parameters of Julia sets to generate a random sequence for the first encryption keys and then uses the Hilbert curve to scramble the initial keys to produce the final encryption keys. By modulo arithmetic and diffuse operation, the final cypher image is created. Hence the key creation in this approach only requires a small number of parameters, which drastically minimises the amount of storage required. Also, the keys have a great sensitivity to even a little disturbance due to the Julia sets' features, such as their infiniteness and chaotic nature.

REFERENCE

[1] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, ‘‘A joint color image encryption and compression scheme based on hyper-chaotic system,’’ Nonlinear Dyn., vol. 84, no. 4, pp. 2333–2356, 2016.

[2] L. Wang, H. Song, and P. Liu, ‘‘A novel hybrid color image encryption algorithm using two complex chaotic systems,’’ Opt. Lasers Eng., vol. 77, pp. 118–125, Feb. 2016.

[3] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, ‘‘Triple chaotic image scrambling on rgb–a random image encryption approach,’’ Secur. Commun. Netw., vol. 8, no. 18, pp. 3335–3345,2015.

[4] Q. Gu and T. Gao, “A novel reversible robust watermarking algorithm based on chaotic system,” D i g. S i g n a l P ro c e s s., vol. 23, no. 5, pp. 213–217, 2013.

[5] H. C. Huang, F. C. Chang, and W. C. Fang, “Reversible data hiding with histogram-based difference expansion for QR code applications,” IEEE Trans. Consumer Electron, vol. 57, no. 2, pp. 779–787, 2011.

[6] Z. C. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Tr a n s . Circuits S y s t . Vi d e o Te c h n o l ., vol. 16, no. 3, pp. 354–362, 2006.

[7] G. Coatrieux, W. Pan, F. Cuppens, and C. Roux, “Reversible watermarking based on invariant image classification and dynamic histogram shifting,” I E E E Trans. I n f. F ore n s i c s S e c u r ., vol. 8, no. 1, pp. 111–120, 2013.

[8] D. Coltuc, “Improved embedding for prediction-based reversible watermarking,” IEEE Trans. Inf . Forensics Secur ., vol. 6, no. 3, pp. 873–882, 2011.

[9] B. Ou, X. Li, Y. Zhao, R. Ni, and Y. Q. Shi, "Pairwise prediction error expansion for efficient reversible data hiding," IEEE Trans . I m a g e Process. vol. 22, no. 12, pp. 5010–5021, 2013.

[10] I. Dragoi and D. Coltuc, "Local prediction based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779–1790, 2014.

[11] S. W. Weng and J. S. Pan, "Reversible watermarking based on eight improved prediction modes," J . I n f . H i d i n g M u l t i m e di a S i g na l P ro c e s s., vol. 5, no. 3, pp. 527–533, 2014.

[12] H. Wu, J. Dugelay, and Y. Q. Shi, "Reversible image data hiding with contrast enhancement," IEEE Signal Process. Lett ., vol. 22, no. 1, pp. 81–85, 2015.

[13] M. Gao and L. Wang, "Comprehensive evaluation for HE based contrast enhancement," A d v . I n t e l l . S y s t . A p p l i c a t ., vol. 2, pp. 331–338, 2013.

[14] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," L e c t u re N o t e s i n C o m p ut e r S c i e n c e, vol. 3304, pp. 115–124, 2005.

[15] L. Xu, Z. Li, J. Li, and W. Hua, ''A novel bit-level image encryption algorithm based on chaotic maps,'' Opt. Lasers Eng., vol. 78, pp. 17–25, Mar. 2016.

[16] X. Wang and H.-L. Zhang, ''A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems,'' Nonlinear Dyn., vol. 83, nos. 1–2, pp. 333–346, 2016.