IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Securing Data Using Cryptography and Steganography

R. Sneha[1], Mrs. K. Vasumathi[2], Dr. S. Selvakani[3]

[1]*PG Scholar, PG Department of computer Science, Government Arts and Science College, Arakkonam, Tamilnadu, India*
[2]*Assistantn Professor, PG Department of computer Science, Government Arts and science College, Arakkonam, Tamilnadu, India*
[3]*Assistant Professor and Head, PG Department of Computer, Science, Government Arts and Science College, Arakkonam, Tamilnadu, India*

Abstract *- One of the preeminent challenges confronting the contemporary digital landscape pertains to the domain of Data Security, a pivotal facet within the realm of information technology. Given the substantial progressions in internet technology, there has been a profound surge in the transfer of voluminous textual and multimedia data across the digital expanse. However, the communication channel facilitating data transmission from sender to recipient is inherently susceptible to breaches.*

In light of the paramount concern surrounding the security of electronic data, both public and private sectors conscientiously employ a diverse array of methodologies and techniques to safeguard information from unauthorized access. Notably, Cryptography and Steganography emerge as the foremost and extensively embraced technologies for ensuring heightened security.

Cryptography, characterized as the art of obfuscating information through encryption, serves to veil the intelligible and significant contents of the data. Simultaneously, Steganography, an adept technique, conceals the very existence of data within a cover medium. This concerted approach addresses the imperative need for both confidentiality and security in the digital milieu.

This paper introduces a security paradigm for safeguarding confidential data, amalgamating three distinct techniques. The initial facet involves image compression, utilizing wavelet transformation to compress the confidential image, thereby diminishing its size. The second facet employs cryptography, specifically relying on symmetric key encryption to obfuscate the confidential image. Lastly, the third facet adopts steganography, employing the least significant bit (LSB) to discreetly integrate the encrypted information within a cover image. Consequently, the overarching objective of this proposed technique is to attain a synthesis of heightened security measures and optimal quality in the reconstruction of the cover image.

Keywords *- Image Steganography; Pixel Value Difference (PVD); Encryption; Decryption; Advance encryption standard (AES)*

1. Introduction

Cryptography and steganography stand as ubiquitous methods employed to fortify communication security [2]. Cryptography, rooted in the mathematical domain, serves as the scientific art of encrypting and decrypting data. Its function is to fortify messages by converting intelligible data (plaintext) into an unintelligible form (ciphertext). The etymology of cryptography derives from the Greek words "kryptós" denoting "hidden" and "gràphin" signifying "writing," encapsulating its essence as "hidden writing" [3, 4]. A cryptosystem encompasses elements such as plaintext, encryption and decryption algorithms, ciphertext, and a key. The plaintext refers to the original, readable form of the message or data, while encryption transforms the plaintext into ciphertext through the utilization of a key. The key controls the cryptosystem and is privy only to the sender and recipient. Decryption, conversely, retrieves the plaintext from the ciphertext [3, 5].

Despite the robust nature of cryptography in securing data, cryptanalysts may succeed in deciphering ciphers by scrutinizing the contents of ciphertext to uncover the plaintext [3]. Cryptographic systems are generally categorized across three distinct dimensions [3]:

A. Nature of Operations on Plaintext

The transformation of plaintext into ciphertext entails two distinct types of operations, each exerting its influence on the original text. The initial mode of operation involves the substitution of each element within the plaintext, whether it be a bit, letter, or a group of bits or letters. This process is characterized by a one-to-one mapping, exemplified by systems such as the Caesar cipher [5].

The second operative paradigm centers on the transposition of characters within the plaintext, orchestrating their interchange based on a predetermined mapping stipulated by the cryptographic key. In this particular operation, the characters in the plaintext retain their original identity but undergo repositioning into different sequences, as exemplified by the Rail Fence cipher. It is noteworthy that many cryptographic systems, denoted as product systems, integrate multiple stages of both substitution and transposition operations to fortify their overall efficacy.

B. Quantity of Utilized Keys

In the context of cryptographic protocols, the quantity of keys employed plays a pivotal role in determining the system's nature. When both the sender and receiver employ a singular key for the encryption and decryption of plaintext, the cryptographic configuration is denoted as symmetric, single key, secret key, or conventional encryption. Symmetric encryption, characterized by its straightforwardness and expeditious processing, involves the use of a shared secret key between the communicating entities.

Conversely, in scenarios where distinct keys are utilized for the encryption and decryption processes – with the sender leveraging a public key and the receiver employing a private key – the cryptographic framework is labeled as asymmetric, two-key, or public key encryption. This methodology introduces a heightened level of complexity and security, as the public key is openly accessible, while the private key is retained exclusively by the intended recipient for decryption purposes.

The paramount concern in the contemporary digital landscape revolves around the security of confidential data. Steganography emerges as a viable solution, constituting an art form wherein confidential data is discreetly concealed within another image, denoted as the cover image [1]. This covert integration renders the confidential data imperceptible to the ordinary user, with only authorized individuals possessing the capability to unveil the hidden information through a prescribed steganographic process.

In parallel, cryptography stands as an alternative security technique, converting secret data into an unreadable format, commonly known as encryption. The inverse process, decryption, restores the unreadable form to its original legible state. Typically, users employ either cryptography or steganography as a singular security approach, recognizing cryptography as a potent and widely utilized technique [2, 3]. The synergy of steganography and cryptography, however, holds significant promise in enhancing security measures within this domain.

The fundamental equation (1) encapsulates a simplistic steganographic method: Cover Image+Secret Data+Key=Stego Image

In this equation, the secret data finds concealment within the cover image, facilitated by a robust key concept such as LSB or MSB, ultimately generating the stego image. The secret data may undergo an additional layer of encryption through cryptography techniques, contingent on the user's chosen conceptual framework [4]. The core objective of the steganographic method remains the discreet embedding of secret data within the cover image, ensuring its invisibility to unauthorized entities [5, 6].

The primary focus of this paper is the formulation and implementation of a secure and efficient symmetric cryptography method to encrypt secret data in conjunction with the steganography method. This proposed cryptographic method assumes a pivotal role in fortifying the user's imperative need for heightened security. The structure of the paper is delineated as follows: Section 2 expounds on related work and offers a comparative analysis of existing methodologies. Section 3 addresses common issues, while Section 4 introduces the proposed work. Section 5 presents a performance analysis of the steganography method in terms of results, and finally, Section 6 provides conclusive remarks.

2. Related work

A.Shoukat [1] stated that numerous methodologies have been employed to ensure data security, utilizing encryption, steganography, or a synergistic amalgamation of both. [1]. The Advanced Encryption Standard (AES), alternatively recognized as Rijndael, constitutes a symmetric-key block cipher.

J. Daemen During the decryption process, the four steps are executed in a reversed sequence. Furthermore, it is noteworthy that the inverse of the mixing column step is excluded from the conclusive round of the decryption phase. The pseudocode encapsulating the Advanced Encryption Standard (AES) is delineated in accordance with the specifications elucidated in reference [2].

F. Omara said that the AddRoundKey operation is applied sequentially to individual columns [3]. This operation involves the amalgamation of a round key word with each column matrix of the state, employing the bitwise XOR operation, as explicated in reference

S. Murphy The merits inherent in the employment of the Advanced Encryption Standard (AES) algorithm encompass heightened security, accommodation of larger key sizes in comparison to the Data Encryption Standard (DES), enhanced swiftness in both hardware and software implementations, cost-effectiveness, and its principal attributes of flexibility and simplicity, as substantiated by reference [4].

A.Sade An alternative technique is posited, departing from the convention of utilizing the First Least Significant Bit (LSB1) in the spatial domain for message bit embedding

within the cover image. Instead, the Third Least Significant Bit (LSB-3) is harnessed to encapsulate the message bits, thereby allowing potential modifications to LSB-1 and LSB-2 as well [5]. Evaluation of this methodology reveals that the LSB-1 approach yields superior Peak Signal-to-Noise Ratio (PSNR) values, indicative of a higher image quality when contrasted with the LSB-3 method. It is noteworthy that the data-carrying capacity remains consistent across both methods. Consequently, the foundational LSB-1 method outperforms the proposed LSB-3 methodology in terms of overall efficacy in reference.

M. Juneja In the discourse outlined in reference [6], an innovative technique has been put forth. The outcomes derived from this technique affirm its heightened security when juxtaposed with alternative methodologies, particularly in its resilience against statistical attacks commonly employed in steganalysis. This resilience emanates from the methodology's adeptness at categorizing images within a user's library according to their appropriateness as cover entities for concealing specific data.

Dutta In the context of reference [7], an innovative approach has been introduced for the covert integration of any encrypted confidential message into a designated cover file. The methodology involves the utilization of two discrete techniques to incorporate a concealed message file within the cover file. Primarily, the secret message file undergoes encryption through the application of both simple bit shifting and XOR operations, thus fortifying its covert nature within the concealment process.

Lather In the scholarly work authored by Yashpal Lather et al., titled "Review Paper on Steganography Techniques" [8], a comprehensive examination is conducted on various steganography methodologies, encompassing their applications and inherent constraints. Furthermore, a meticulous distinction is drawn between the domains of steganography and cryptography. The discourse extends to the inclusion of textual as well as diverse image steganography techniques within the purview of this scholarly exposition. Ultimately, the deduction posited is that steganography employing a cryptographic key manifests superior security attributes when juxtaposed with non-key steganographic methodologies.

Bonny In the scholarly work authored by Bonny et al., as presented in reference [9], the discourse revolves around the meticulous examination of "Feature-based image stitching algorithms." This scholarly investigation delves into the intricacies of the image stitching technique, elucidating its essential tripartite progression involving calibration, registration, and blending. Moreover, a discerning analysis is undertaken, spotlighting the direct technique and the feature-based technique as the principal paradigms within the realm of image stitching. The paper further expounds upon the merits and demerits inherent in the domain of feature-based image stitching techniques.

Shaik Akbar In the scholarly treatise authored by Shaik Akbar et al., featured in citation [10] under the appellation "Bit-Plane Slicing Algorithm for Crime Data Security using Fusion Technologies," a pioneering system is postulated. This system seamlessly integrates the disciplines of Forensic Science and Steganography, culminating in a sophisticated hybrid technology meticulously designed for safeguarding criminal data. The employed methodology involves the utilization of crime person fingerprints as concealment vectors for the data. These fingerprints undergo a meticulous segmentation process, employing a bit-plane slicing algorithm that partitions them into eight distinct slices. Subsequently, official crime data is discreetly embedded within one of these eight slices. The principal objective of this scholarly endeavor is to ensure the impregnable security of criminals' data ensconced within their unique fingerprints.

3. Methodology

3.1. Encryption

- Input Message: The original message that needs to be kept confidential.
- Encryption Algorithm**:** Apply a cryptographic algorithm (e.g., AES, RSA) along with a secret key to encrypt the message.
- Encrypted Message: The result of the encryption process.
- Output: The output includes Cipher message and key.

3.2. Embedding the message:

- Input: The user needs to provide an image that can be either color or greyscale image.
- Processing: The processing is done in two steps.
- 2D-DWT-3L can be formulated as a consecutive transformation using low-pass and high-pass filters.
- Read the value of the pixel, convert it to its equivalent binary form and modify the least significant bit accordingly.

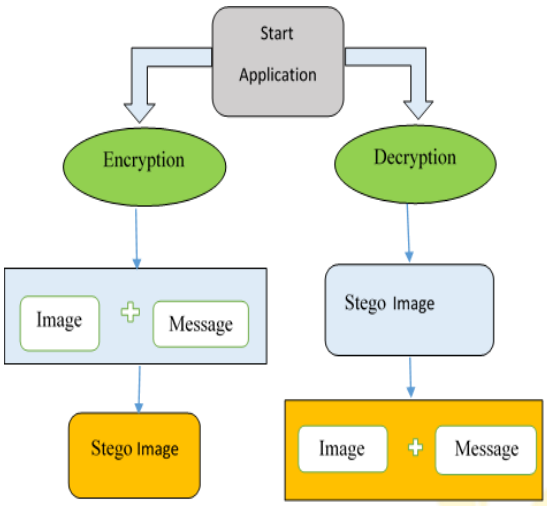

Fig 1: Steps in the project the various steps in the system are as shown above in the flowchart.

Certainly, I'll provide a general explanation of embedding a message, which typically involves hiding or encoding information within another medium. This can be achieved through various techniques, including cryptography, steganography, or a combination of both as shown in Fig 1.

A. Cryptography

Encryption: This involves converting the original message (plaintext) into a scrambled format (ciphertext) using an encryption algorithm and a secret key. The encrypted message appears as random data and is unreadable without the corresponding decryption key.

Decryption: The recipient, who possesses the decryption key, can reverse the process, converting the ciphertext back into the original plaintext and revealing the intended message.

B. Steganography

Concealment: Steganography is the art of concealing information within another medium in such a way that the presence of the hidden information is not obvious. This is different from cryptography, which focuses on making the message unreadable. In steganography, the goal is often to make the existence of the message undetectable.

Technique: Steganographic techniques can include hiding information within images, audio files, text, or other types of data. For example, one common method is to alter the least significant bits of pixel values in an image to encode the hidden message without significantly altering the image's appearance.

Extraction: The recipient, who is aware of the steganographic method used, can extract the hidden information from the carrier medium.

Combined Approach (Encryption + Steganography):

Encrypting the Message: Before embedding, the message is encrypted to add an extra layer of security. Even if an unauthorized party detects the hidden information, they would need the decryption key to make sense of it.

Embedding the Encrypted Message: The encrypted message is then embedded using steganographic techniques. This can be done in a way that is visually or perceptually inconspicuous, making it difficult for an observer to realize that there is hidden information.

Recovery: To recover the original message, the recipient first extracts the hidden, encrypted information using steganography techniques and then decrypts it using the appropriate decryption key.

This combined approach enhances the security of the communication, as it requires both knowledge of the steganographic method and possession of the decryption key to access the meaningful content.

3.3 Extracting the message

- Input: Stego image
- Processing: Scan the image row by row and compute the 2D wavelet for the first, second, and third levels by haar filter.
- Extract the text embedded in vertical coefficients of odd and even values. Compute idwt2 that generates the original image.
- Output: Retrieved secret message and original cover image.

3.4 Steganography Extraction:

- Purpose: Reveal hidden information within a carrier medium.
- Techniques: Employ steganographic methods like LSB (Least Significant Bit) extraction, frequency domain analysis, or visual/audio pattern recognition as shown in Fig 2.
- Objective: Retrieve the concealed message without altering the carrier medium significantly.

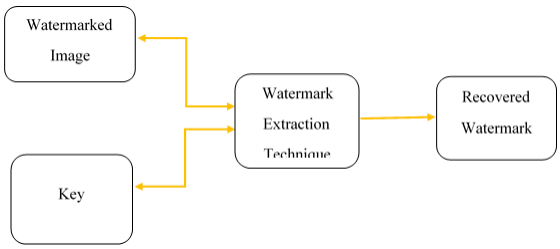

Fig 2: Extracting Message

3.5 Decrypting the message

- Input: The receiver needs to provide the private key.
- Processing: The cipher text is divided into two parts i.e., Hashed Text and Hashed Key. Decompress both parts and split and decrypt into odd and even parts.
- If odd insert odd characters into odd indices within the main message.
- Else Insert even characters into even indices within the main message. Output: The output includes the secret message.

4. Experiment and Results

4.1. Experimental Setting:

The operational platform utilized herein is a computing system running Windows 8, fortified with an authentic Intel(R) Core(TM) i5-4210U CPU operating at 1.70 GHz and 240 GHz, complemented by an 8 GB RAM module. The algorithmic implementation is facilitated through Python, employing the associated Python code.

4.2. Comparative Standards:

A series of experiments were conducted utilizing standardized grayscale images of dimensions 512 * 512 and 256 * 256, featuring iconic subjects such as Cameraman, Lena, Peppers, Lake, Airplane, and Baboon. The integration of a text encrypted message transpired subsequent to the initial encryption via the AES-MPK algorithm, followed by concealment employing the PVD-MSLDIP-MPK algorithm for transmission. Upon reception, the concealed message underwent extraction, succeeded by decryption.

4.3. Assessment Metrics:

The efficacy of the amalgamated algorithm is appraised through the quantification of imperceptibility (Stego-image quality) and payload (hiding capacity). Imperceptibility, indicative of the disparity induced by data embedding in the original cover, is gauged by the stego-image quality, with a higher value denoting greater invisibility of the concealed message. Payload, or hiding capacity, signifies the volume of concealed data within a cover image without perceptible degradation in image quality. Noteworthy is the caveat that concealing a substantial amount of data, resulting in overt distortion, holds no significance. A steganographic technique is deemed advantageous if it augments payload while preserving an acceptable visual quality of the stego-image or enhances stego-image quality while maintaining or improving hiding capacity. The outcomes derived from these experiments are meticulously documented and synthesized in Tables [1, 2, 3].

TABLE 1. PROPOSED ALGORITHM WITH DIV=19

Cover Image 256*256	Hiding Capacity (bytes)	PSNR of Method in [21]	Hiding Capacity (bytes)	PSNR of Proposed Method
Baboon	18.616	33.80	18.624	41.7875
Lena	13.003	43.56	13.008	44.9864
Pepper	16.394	36.91	16.400	43.6845

Table 1 elucidates a meticulous comparative analysis between the envisaged integrated technique and the approach delineated, encompassing the clandestine embedding of (18.616, 13.003, and 16.394) secret bytes within 256 x 256 cover images of Baboon, Lena, and Peppers, respectively. The outcomes manifest an elevation in Peak Signal-to-Noise Ratio (PSNR) values for the proposed method with the PSNR values transcending the 36 dB threshold. This substantiates the commendable aptness of the proposed methodology.

Depicts a visual juxtaposition between the resultant stego images and their corresponding histograms against cover images and their histograms. Evidently, the stego histograms and visual quality of the resultant stego-image exhibit inconspicuous alterations. Furthermore, the modification in histograms is contingent upon the inherent attributes of the image, namely the juxtaposition of smooth and edge areas. A discernible correlation is observed wherein images characterized by a heightened prevalence of edge areas, such as Baboon and Lena, exhibit more conspicuous alterations in stego histograms compared to Pepper image. Noteworthy is the influence of the MPK_PVD method employed in concealing information within smooth areas.

TABLE 2. COMPARISON OF PAPER [22] WITH THE PROPOSED METHOD WITH DIV=19

Cover Image 512x512	Hiding capacity (bytes)	PSNR of method in [22]	Hiding capacity (bytes)	PSNR of Proposed method
Baboon	57.043	39.2	63.408	42.8113
Boat	52.490	41.0	62.576	44.5444
Lake	52.662	41.5	62.672	44.0388
Lena	50.894	43.4	62.208	44.9678
Peppers	50.815	42.5	62.000	44.8326

Table 2, meanwhile, scrutinizes the proposed methodology against the framework, incorporating the covert embedding of (63.408, 62.576, 62.672, 62.208, and 62.000) secret bytes within 512 x 512 cover images of Baboon, Boat, Lake, Lena, and Peppers, respectively. The findings corroborate the superiority of the proposed method in terms of PSNR values when juxtaposed with the approach advocated, notwithstanding the application of a greater hiding capacity.

TABLE III. LISTING OF COVER IMAGES AND SECRET MESSAGES WITH THE TIME REQUIRED TO ENCRYPT, HIDE, EXTRACT, AND DECRYPT OF SECRET MESSAGE

Cover Image		Secret Message (Bytes	Time (Seconds)			
Name	Size		Encrypt	Hide	Extract	Decrypt
Lena	256*256	144	4.28	0.01	0.02	4.67
Pepper	256*256	416	12.31	0.03	0.04	13.72
Baboon x	256*256	992	30.01	0.17	0.10	32.34
Cameraman	512*512	1.744	50.43	0.09	0.19	55.96
Boat	512*512	2.720	81.42	0.15	0.29	89.01
Airplane	512*512	3440	101.1	0.17	0.49	106.3

This attests to the enhanced quality of the stego-image and augmented hiding capacity, thereby underscoring the efficacy and suitability of the proposed methodology.

5. Future work

The In forthcoming endeavors, we eagerly anticipate the exploration of the application of the proposed methodology to both auditory and visual domains. Additionally, we aspire to augment the aforementioned approach, striving to amplify its capability beyond its current threshold, while concurrently maintaining, if not surpassing, the same Peak Signal-to-Noise Ratio (PSNR).

This paper introduces a novel secure communication paradigm, amalgamating cryptographic and steganographic methodologies to establish a dual layer of security. This stratagem ensures that the steganalyst remains unable to discern the plaintext unless possessing the requisite secret key for decrypting the ciphertext. Initially, the confidential data undergoes encryption utilizing the Advanced Encryption Standard with Modified Public Key (AES_MPK). Subsequently, the encrypted data is clandestinely embedded within a grayscale image, employing the PVD-MPK and MSLDIPMPK techniques. This synergistic integration permits the transmission of confidential data through open channels, as the ciphertext assumes a non-arbitrary appearance, obfuscated by steganography within the images.

Empirical findings affirm that our proposed model surpasses extant methods in concealing a more substantial volume of information, concurrently elevating the visual quality of the resultant steganographic image. Notably, the model proves efficacious for covert data communication. In future endeavors, we aspire to extend the application of the proposed method to encompass audio and video modalities. Additionally, our focus will be directed towards augmenting the model's capacity while maintaining, or ideally surpassing, the extant Peak Signal-to-Noise Ratio (PSNR).

6. Conclusion

This scholarly work directs its attention towards a myriad of methodologies employed in the safeguarding of data. Each method boasts its own set of merits and demerits, with the applicability of distinct techniques contingent upon the diverse domains of their application. Paramount among the universal parametric prerequisites are security, robustness, imperceptibility, and capacity.

Divergent techniques exhibit varying proclivities towards these parametric requirements, leading to a nuanced landscape where some methods surpass others in security, while others excel in accommodating larger data hiding capacities. The spectrum extends to the resilience of techniques against assorted attacks, with certain methodologies proving more impervious, juxtaposed with others that manifest fragility.

Complexity becomes an additional facet to consider, as some techniques, despite their intricacy, strike a harmonious balance by ensuring security, while others, although more straightforward, may lag behind in terms of safeguarding efficacy. Consequently, a pervasive theme emerges, wherein the optimization of one parameter invariably necessitates trade-offs with others.

In addressing this intricate challenge, the incorporation of combined techniques emerges as a judicious solution, affording the opportunity to synergize disparate approaches. This strategic amalgamation not only harmonizes the various parametric requirements but also endeavors to achieve an optimal equilibrium, ensuring maximal security for the safeguarding of data.

The envisaged model constitutes a synthesis of Cryptography and Steganography, with its principal objective being the fortification of data against unauthorized access while concurrently mitigating the risk of adversarial incursions during the transmission process. The dual-layered security paradigm augments the overall safeguarding of information. Its applications span diverse sectors such as banking, defense, among others.

Notably, the data concealment capabilities within audio and video formats surpass those inherent in images. This propels the prospect of employing audio or video steganography in conjunction with cryptography, facilitating the seamless transmission of voluminous data across public networks without succumbing to security breaches.

References

[1] A. Shoukat et al "A Survey about the Latest Trends and Research Issues of Cryptographic Elements," IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, PP. 140-149, May 2011.

[2] J. Daemen, and V. Rijmen "AES Proposal: Rijndael," version 2, PP. 1- 45, 1999, Available in http://csrc.nist.gov/archive/aes/rijndael/Rijndaelammended.pdf#page=1.

[3] R. H. Sakr, F. Omara, and O. Nomir, "A COMPARATIVE STUDY OF SECURITY ALGORITHMS FOR CLOUD COMPUTING," International Journal of Intelligent Computing and Information Science, Vol.13, PP. 73-84, OCTOBER 2013.

[4] *S. Murphy, "The Advanced Encryption Standard (AES)," information Security Technical Report, Vol. 4, No. 4, PP.12-17, 1999.*

[5] I. A. Sada, "Hiding Data Using LSB-3", J.basrah researches (sciences), vol. 33. No. 4, pp. 81-88, Dec. 2007.

[6] M. Juneja, and P. S. Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," International Conference on Advances in Recent Technologies in Communication and Computing, PP. 302-305, 2009

[7] Dutta et al, "New Data Hiding Algorithm in MATLAB using Encrypted secret message," International Conference on Communication Systems and Network Technologies, PP. 262-267, 2011

[8] *Lather, Yashpal, Megha Goyal, and Vivek Lather. "Review Paper on Steganography Techniques." IJCSMC, Signal Processing 4.1 (2015): 571-576.*

[9] *Bonny, Moushumi Zaman, and Mohammad Shorif Uddin. "Feature-based image stitching algorithms." 2016 International Workshop on Computational Intelligence (IWCI). IEEE, 2016,*

[10] *Shaik Akbar, Dr K., and T. Anand. "Bit-Plane Slicing Algorithm for Crime Data Security using Fusion Technologies."*