# A Survey on Different Ways of Secure Image Transmission

Ankita P. Pande[1], Dr. Nileshsingh V. Thakur[2]

[1]*M.E. Student, Department of Computer Science & Engineering, PRCEAM, Badnera, India.*
[2]*Principal and Professor, Department of Computer Science & Engineering, PRCEAM, Badnera, India.*

**Abstract** - *Nowadays, nearly every individual in the world are connected to every other using Internet. Different types of images are transmitted through Internet for various applications. These images usually contain either confidential or private data. Therefore, ensuring confidentiality, integrity, authentication and non-repudiation of images during transmission is an important issue. During data transmissions, these highly confidential data can be manipulated by an unauthorized person, thus leading to an insecurity for its sender. To overcome this problem, many techniques have been proposed, in which data hiding and image encryption are the two main techniques. In this paper, different image security techniques are surveyed and summarized in the tabular form. In this summary table we have covered various parameters such as basic concept used by the author, types of images used, performance evaluation parameters, author's remark about their work and lastly our findings on their work.*

**Key Words:** Cryptography, Image Transformation, Image Encryption, Image Decryption, Data Hiding.

## 1. INTRODUCTION

The security of images has become increasingly important due to rapid growth of the Internet. Number of images are transmitted through the web for various usages such as satellite images, medical imaging systems, military database and services, broadcasting, banking, confidential enterprise archives, etc. Therefore, it is essential to protect the confidentiality of images by securing sensitive information from intruder. This can be achieved by converting the original image to other non-understandable form before sending it to the receiver by using technique called image encryption or by using data hiding technique which hides the existence of that images from the unauthorized user.

At present, numerous image encryption methods are available to keep unauthorized users away from sender's transmitted images. Most of the existing encryption algorithms are commonly used for text data, but algorithms that are good for text data may not be suitable for image because of their large size and real time constraints. Another technique for providing image security is data hiding. A main problem of the data hiding method in images is the difficulty in inserting a large amount of data into a cover image. Specially, if a secret image and a cover image is of the same size. Image transformation is also used for providing security to an image during transmission. The information presents in digital image is due to the correlation between two adjacent image pixels. This perceivable information can be decreased by reducing the pixels correlation using certain transformation process.

Many techniques are available for securing images and different techniques provides different level of image security, which can be calculated based on different evaluation factors. In order to evaluate the performance of different image security techniques, the standard evaluation parameters like pixels correlation, entropy value, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Histogram analysis, Unified Average Changing Intensity (UACI), Number of Pixel Change Rate (NPCR), etc. are considered.

## 2. LITERATURE REVIEW

There are many techniques for securing images. In this paper, few of the prominent existing research work are reviewed to cover all the available image security techniques such as image transformation, image encryption, and image steganography.

### 2.1 Image Transformation

In image transformation, digital image is taken as an input and produces another image as its output to enhance the security level of an image. The first image encryption method we have discussed in the below table is block-based image transformation [1], [2]. It divides input image into blocks, which were rearranged into a transformed image using their respective transformation algorithm. Their results show's that increasing the number of blocks by dividing image into smaller blocks results in a lower correlation and higher entropy. Another type of image transformation like Fractional Fourier Transformation (FRFT) and wavelet transform [3], [4] are also covered in the following table.

### 2.2 Image Encryption

Image encryption is the process of converting an input image into another random image that is hard to understand. This can be done by using key or without key. There are numerous image encryption methods available to make transmission of images more secure. Different types of image encryption methods are discussed below.

**2.2.1 Private Key Image Encryption:** Private key image encryption also called as symmetric key encryption or conventional encryption. It uses the same shared key for image encryption and decryption. Hence, image security is mainly dependent on key length in private key cryptography. The sender encrypts the image using secret key and sends to the receiver while the receiver decrypts the image using the same shared key to obtain the original image. However, before transmitting encrypted image, it is necessary that both the sender and the receiver agree upon the key and no one other than these two should know about it. Various private key encryption methods [5]–[7] are reviewed in the following table.

**2.2.2 Public Key Image Encryption:** Public key image encryption also called as an asymmetric image encryption [8], [9]. It involves pair of keys for an image encryption and image decryption. If sender wants to transfer image to the receiver, then sender has to encrypt image using receiver's public key and receiver will decrypt the image using its own private key. Therefore, private key encryption technique is significantly faster than public-key encryption technique. Hence, typically used in bulk data encryption.

**2.2.3 Chaos Based Cryptography:** Chaos based cryptography [10], [11] is a study of nonlinear dynamic system in which chaos denotes the randomness. This chaotic method are mostly sensitive to initial conditions and other system factors. Because of the sensitiveness, the chaotic system acts very randomly. The main advantages of chaos based cryptography are its high flexibility in the design of encryption technique, availability of very large number of chaotic system's variants, and numerous probable encryption keys.

**2.2.4 Selective Image Encryption:** Selective image encryption [12], [13] also called as partial image encryption. It is a method of encrypting only the portions of an image. This approach minimizes the execution time of an encryption as it encrypts only a part of the image and hence increases performance. Real time applications mainly requires this type of technique.

**2.2.5 Image encryption using compression and encryption:** There are mainly three ways of achieving image security using this approach, the first way is compression followed by encryption, second way is encryption followed by compression and last is joint compression and encryption. Encryption and compression [14]–[18] are used to provide high-level of image security and to reduce the size of an encrypted images resp. The order of compression and encryption can vary. Different authors have claimed different views regarding the ways of using this combined approach. Some authors did compression followed by encryption, while others first encrypted image, then compressed. For fast processing and improved image security, joint compression and encryption is also used.

**2.2.6 Visual Cryptography:** Visual cryptography [19], [20] was first proposed by Moni Naor and Adi Shamir in 1994. It is mainly used for biometric security, watermarking, remote electronic voting, etc. Visual cryptography encrypts visual information (picture, text, etc.) into *n* transparent images (shares) and person having all *n* shares can perform the decryption visually without mathematical calculations and also without the help of computers. Any person having n-1 shares cannot reveal information about the original image.

**2.2.7 Keyless approach:** Keyless approach [21] of image encryption is designed to overcome the limitations of key oriented techniques such as high computational cost in encryption process, maintaining the key records. The keyless approach of reversible color image encryption is reviewed in the following table.

### 2.3 Image Steganography

Steganography is a data hiding technique used to protect multimedia data. It hides information within other information to make it impossible for any unauthorized user to identify presence of any secret information. Steganography uses different types of carriers like text, digital image, or video, of which digital images are the most popular. Image steganography works slightly different from that of image cryptography. The cryptography keeps the contents of a message secret whereas the steganography keeps the existence of a message secret. We have analyzed and tabulated various image steganography approaches [22]–[24] used for securing images.

### 2.4 Other Techniques for Image Security

Nowadays, many new methods for improving the security level of images have been proposed and every day new image security technique is evolving. Some of these techniques [25]–[29] are summarized in the following table.

**Table-1:** Summary of different image security techniques.

| Authors | Images used | Concept used | Performance evaluation parameter | Authors remark | Our findings |
|---|---|---|---|---|---|
| Mohammad Ali Bani Younes and Aman | BMP image of size 300 pixels x 300 pixels with 256 | Combination of block-based image transformation and | 1. Correlation<br>2. Entropy | 1. High security level of the encrypted images compared to using the Blowfish alone and results in lower correlation and | Transformation table has complex structure. |

| | | | | | |
|---|---|---|---|---|---|
| Jantan [1] | colors | Blowfish encryption. | | higher entropy value.<br>2. Enhancing the number of blocks resulted in better image security. | |
| Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma [2] | BMP and JPEG image of size 300 pixels x 300 pixels with 256 colors | An image encryption approach using a combination of image permutation technique followed by a new encryption algorithm called “Hyper Image Encryption Algorithm” (HIEA). | 1. Entropy<br>2. CPU utilization<br>3. Memory utilization | 1. 70% better entropy.<br>2. 80% better efficiency.<br>3. Maximal security. | Achieved higher entropy for same image than [1], hence efficient than [1]. |
| Ran Tao, Xiang-Yi Meng, and Yue Wang [3] | Grayscale image of “Lena” with a size of 256 x 256 | Image encryption by multiorders of FRFT. | 1. MSE | 1. Larger key space and the quantity of keys can be set as large as two times the amount of the pixels in the original image.<br>2. Image decryption is very sensitive to the deviations in the transform orders. | Security level of the image can be enhance by using the proposed method with other image encryption methods. |
| Kevin Sean Chan, and Faramarz Fekri [4] | Grayscale image of Lena | A new two-round private key wavelet cryptographic system. | 1. Computational complexity | 1. Authors introduced the first application of finite-fields wavelets to cryptography.<br>2. Proposed approach has equal computational complexity to AES and nearly half the complexity of DES. | Scope of developing characteristics, which limit different attacks. |
| Dr. J. Abdul Jaleel and Jisha Mary Thomas [5] | A grayscale image of Lena in PNG format and a color image of a cute baby in JPG format | A Symmetric key cryptographic technique called Blowfish algorithm using a key of variable size up to 448 bits. | 1. Pixel correlation | Better than other symmetric key algorithms as it uses a variable-length key from 32-bits to 448-bits. | The Blowfish algorithm is strong and resistant to hacking as it encrypts the data by a 16 round function iterating Feistel network. |
| Narinder Kaur and Kumar Saurabh [6] | Grayscale images | A new symmetric image encryption algorithm using combination of chaotic maps and pseudorandom numbers. | 1. Cross Correlation<br>2. Entropy<br>3. Histogram Analysis | Proposed approach is protected and proficient for ciphering an image. | Proposed approach is efficient as capable of encrypting real-time images. |
| Nandeesh G S, Vijaya P A, and Sathyanarayana M V [7] | Grayscale images | An image encryption approach based on confusion-diffusion design. | 1.Correlation<br>2. Histogram analysis<br>3. NPCR<br>4. UACI | The proposed scheme leads to an improved security level in terms of UACI, NPCR and entropy of the cipher-images. | Stands good against differential attack. |
| Abdullah M. Jaafar and Azman Samsudin [8] | A black and white secret image | A low computational public-key image encryption method based on non-expansion visual cryptography and Boolean operations. | 1. Computational complexity | Proposed approach can encrypt and decrypt image easily without complex computations. | Requires less computation than other public-key encryption schemes. |
| Jayant Kushwaha and Bhola Nath Roy [9] | All types of images | A public key cryptography algorithm using a combination of pixel encryption and block encryption. | 1. Correlation<br>2. Entropy | The correlation between image pixels is reduced and entropy is increased by using proposed technique. | The encryption and decryption process is convenient for the users. |
| Jakimoski G and Kocarev L [10] | Not mentioned | Presented several block encryption ciphers based on chaos by using exponential and logistic maps. | 1. Differential and linear cryptanalysis | They show that their ciphers are resistant to known attacks. | Ciphers can be crack by brute force attack. |
| Mayank Mishra, | Color images | An image encryption | 1. Correlation | Shows a good resistance against | Proposed approach |

| | | | | | |
|---|---|---|---|---|---|
| Prashant Singh, and Chinmay Garg [11] | | algorithm using a combination of pixel scrambling and three chaotic maps. | | statistical attacks and brute-force. | provides good efficiency and also useful for real time image encryption and transmission. |
| Sapna Sasidharan and Jithin R [12] | Grayscale images of size 512×512 | A selective image encryption using Discrete Cosine Transform (DCT) with Rivest Cipher 4 (RC4) stream cipher. | 1. PSNR<br>2. Histogram analysis<br>3. Entropy | Proposed approach results in low PSNR values of the encrypted image and are resistant to statistical attacks. | Provides better image security. |
| Upendra Bisht and Shubhashish Goswami [13] | RGB image | A selective image encryption technique for easy and fast partial encryption of images through MATLAB. | 1. Histogram analysis | Proposed approach is easy to understand and can be easily implemented using MATLAB. | Proposed approach provides average image security level. |
| Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang [14] | Grayscale images such as Lena, Peppers, Goldhill, Boat, Man, Harbor, Airplane, Barbara, Bridge, Tank | Permutation based image Encryption-then-Compression (ETC) system. | 1. PSNR | 1. Effective in destroying the semantic meaning of the images. | The proposed compression approach applied to encrypted images is slightly worse in terms of compression efficiency. |
| Abdul Razzaque & Nileshsingh V. Thakur [15] | Three standard gray level images. Lena.bmp Mandril.tiff and Boat.gif | Image encryption using private key cryptography and compression using DCT. | 1. PSNR<br>2. Coding/decoding time | The compression ratio of the proposed approach using DCT is constantly 8, regardless the format of the input image. | Both security and bandwidth requirements are satisfied. |
| Xiangui Kang, Anjie Peng, Xianyu Xu, and Xiaochun Cao [16] | 8-bit grayscale images of size 512×512 | A scalable lossy compression method for pixel encrypted images. | 1. PSNR | Proposed method achieves better performance than the existing lossy compression method for pixel-value encrypted image. | Compression of encrypted video is not possible with this approach. |
| Philip P. Dang and Paul M. Chau [17] | Tiffany and San Diego grayscale image | Combined image compression-encryption technique using Discrete Wavelet Transform (DWT) and Data Encryption Standard (DES) resp. | 1. PSNR<br>2. MSE | Enhances image security during transmission and also improves the transmission rate. | Results can be improved by using DWT technique of image compression with other image encryption techniques. |
| Abdul Razzaque and Dr. Nileshsingh V.Thakur [18] | Standard<br>gray level images of size 512×512 like Lena.bmp, Boat.gif,<br>Lena.tif, Jetplane.gif and Mandril.tif | Image compression with partial encryption<br>without sharing the secret key. | 1. Compression ratios<br>2. PSNR | Image can be encrypted and decrypted without sharing secret key. | Image transmission time is balanced by using partial encryption algorithm. |
| In Koo Kang, Gonzalo R. Arce, and Heung-Kyu Lee [19] | Original images Lena and Baboon of size 256×256, Baboon, Pepper, and Flower of size 384×256 in natural colors are provided for the share generation | A visual information pixel (VIP) synchronization and a color visual cryptography encryption using error diffusion. | 1. PSNR | VIP synchronization holds the pixels positions carrying visual data of original images throughout the color channels and error diffusion creates shares pleasant to human eyes. | This approach enhances the visual quality of the decrypted image. |
| Xiang Wang, Qingqi Pei, and Hui Li [20] | Binary images | An extended tagged visual cryptography (TVC) method, called as lossless TVC (LTVC). | 1. Image quality of the decoded image | Proposed method have successfully overcome the limitations of TVC. | The LTVC gives the better performance than TVC. |
| Prof. Pragati Patil, Prof.Vinod Nayyar, and Pratibha S. Ghode [21] | RGB bmp images | An enhanced keyless approach for image encryption in lossless RGB images. | 1. PSNR | Proposed approach can ensure the lossless transmission of images. | Keyless approach removes the problem of maintaining the key records and also reduces high computational cost. |

| | | | | | |
|---|---|---|---|---|---|
| Der-Chyuan Lou and Chia-Hung Sung [22] | Grayscale images | Chaotic asymmetric steganographic (CAS) approach based on a chaotic dynamic system and the Euler theorem. | 1.PSNR<br>2.Computational cost | 1. No visual artifacts occur between the stego-images and the original images. | This approach can be extended to color images. |
| K. Satish, T. Jayakar, Charles Tobin, and K. Madhavi and K. Murali [23] | Test images of Lena, Barbara, Peppers and Bird each of size 256x256 (64 kB) | A chaos based spread spectrum image steganography (CSSIS) method using three keys. | 1. Stegosignal Power (db)<br>2. Steganographic SNR<br>3. Embedded Signal BER<br>4. Message<br>Payload (bpp) | 1. Cheap implementation due to the combination of chaotic encryption and modulation.<br>2. Achieved robustness by interleaving the message using a chaotic sequence. | Provides good security as message is secured by using three keys. |
| Bingwen Feng, Wei Lu, and Wei Sun [24] | The 5000 original bitmap format binary images consist of cartoon, CAD, texture, mask, handwriting, and document images | A spatial domain-based binary image steganographic method for minimizing the embedding distortion on the texture. | 1. Distance-Reciprocal Distortion<br>2. Eld Distortion | This proposed steganographic scheme can produce stego images with better qualities when the same length of data bits are embedded. | Used for protecting only bitmap images. |
| I. J. Lai and W. H. Tsai [25] | Color images and text-type grayscale document images | Secret-fragment-visible mosaic image. | 1. RMSE | Proposed approach is good for covert communication. | Space complexity is high as it needs target image database. |
| Ya-Lin Lee and Wen-Hsiang Tsai [26] | Color images | Secret-Fragment-Visible_Mosaic images using nearly reversible color transformations. | 1. RMSE<br>2. MSSIM | 1. Solved the difficulty of hiding a large amount of message data into the cover image.<br>2. No need of a target image database. | Resolved the weakness of Lai and Tsai [25]. |
| Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux [27] | 100 ultrasound images of 576 × 690 pixels of 8-bit depth, and 200 PET images of 144 × 144 pixels of 16-bit depth | A combined image watermarking and image encryption approach for protecting medical images. | 1. PSNR<br>2. Entropy | 1. It guarantees a priori and a posteriori security of medical images.<br>2. Results in low distortion in the retrieved image and high capacity is achieved. | The proposed approach has high complexity and less robust to lossy image compression attack. |
| Ching-Nung Yang, Chih-Cheng Wu, Yi-Chin Lin, and Cheonshik Kim [28] | Black and white images | (2,n) matrix-based secret image sharing (MSIS) method based on binary matrix operations. | 1. Histogram analysis | 1. Satisfies the threshold property.<br>2. Low computational complexity of image recovery. | Security is enhanced using proposed method. |
| Subramania Sudharsanan [29] | Color and monochrome images of JPEG or other image formats | A new {2,2} shared encryption method for images. | 1. Computational complexity | Proposed approach can be extended to any other transform or wavelet domain techniques for image coding. | This can be extended to a {*n*,*k*} sharing scheme with relatively simpler additional steps. |

## 3. CONCLUSION

Preserving image security has become an important issue since transmission of images over the Internet occur very frequently. In this paper, we have surveyed different image security techniques including conventional image encryption technique. There are numerous image encryption techniques presented in the mid of 1990s and each technique is unique in a certain way. Particular image encryption technique provides good image quality at receiver side while other provides degraded images, also certain image encryption techniques have less processing speed while other has high processing speed. In this paper, all of these properties of varies image encryption techniques are reviewed and presented in tabular form. Other techniques of image security are also surveyed in this paper.

## REFERENCES

[1] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, vol. 35, no. 1, pp. 15-23, Feb. 2008.

[2] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric

Transformation Algorithm (Hyper Image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering, vol. 1, no. 3, pp. 7–13, Dec. 2011.

[3] Ran Tao, Xiang-Yi Meng, and Yue Wang, "Image Encryption With Multiorders of Fractional Fourier Transforms", IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 734–738, Dec. 2010.

[4] Kevin Sean Chan, and Faramarz Fekri, "A Block Cipher Cryptosystem Using Wavelet Transforms Over Finite Fields", IEEE Transactions on Signal Processing, vol. 52, no. 10, pp. 2975–2991, Oct. 2004.

[5] Dr. J. Abdul Jaleel and Jisha Mary Thomas, "Guarding Images using a Symmetric key Cryptographic Technique: Blowfish Algorithm", International Journal of Engineering and Innovative Technology, vol. 3, no. 2, pp. 196–201, Aug. 2013.

[6] Narinder Kaur and Kumar Saurabh, "An Efficient Image Encryption System", International Journal of Engineering Science and Innovative Technology, vol. 3, no. 4, pp. 139–142, Jul. 2014.

[7] Nandeesh G S, Vijaya P A, and Sathyanarayana M V, "Image Encryption Using Bit-Level Sub Image Blocks Confusion and Circular Diffusion", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 185–193, May 2013.

[8] Abdullah M. Jaafar and Azman Samsudin, "A New Public-Key Encryption Scheme Based on Non-Expansion Visual Cryptography and Boolean Operation", International Journal of Computer Science, vol. 7, no. 2, pp. 1–10, Jul. 2010.

[9] Jayant Kushwaha and Bhola Nath Roy, "Secure Image Data by Double encryption", International Journal of Computer Applications, vol. 5, no. 10, pp. 0975–8887, Aug. 2010.

[10] Jakimoski G and Kocarev L, "Chaos and cryptography: block encryption ciphers based on chaotic maps", IEEE Transactions on Circuits and Systems, vol. 48, no. 2, pp. 163–169, Feb. 2001.

[11] Mayank Mishra, Prashant Singh, and Chinmay Garg, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal of Information & Computation Technology, vol. 4, no. 7, pp. 741–746, 2014.

[12] Sapna Sasidharan and Jithin R, "Selective Image Encryption Using DCT with Stream Cipher", International Journal of Computer Science and Information Security, vol. 8, no. 4, pp. 268 – 274, Jul. 2010.

[13] Upendra Bisht and Shubhashish Goswami, "Analysis and Implementation of Selective Image Encryption Technique Using Matlab", Journal of Computer Engineering, vol. 16, no. 3, pp.108–111, Jun. 2014.

[14] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 39–50, Jan. 2014.

[15] Abdul Razzaque & Nileshsingh V. Thakur, "An Approach to Image Compression and Encryption", International Journal of Image Processing and Vision Sciences, vol. 1, no. 2, 2012.

[16] Xiangui Kang, Anjie Peng, Xianyu Xu, and Xiaochun Cao, "Performing scalable lossy compression on pixel encrypted images", EURASIP Journal on Image and Video Processing, 2013.

[17] Philip P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications", IEEE Transactions on Consumer Electronics, vol. 46, no .3, pp. 395–403, Aug. 2000.

[18] Abdul Razzaque and Dr. Nileshsingh V.Thakur, "An Approach to Image Compression with Partial Encryption without sharing the Secret Key", IJCSNS International Journal of Computer Science and Network Security, vol. 12, no. 7, Jul. 2012.

[19] In Koo Kang, Gonzalo R. Arce, and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on Image Processing, vol. 20, no. 1, pp. 132–145, Jan. 2011.

[20] Xiang Wang, Qingqi Pei, and Hui Li, "A Lossless Tagged Visual Cryptography Scheme", IEEE Signal Processing Letters, vol. 21, no. 7, pp. 853–856, Jul. 2014.

[21] Prof. Pragati Patil, Prof.Vinod Nayyar, and Pratibha S. Ghode, "A Keyless approach to Lossless Image Encryption", vol. 4, no. 5, pp. 1459–1467, May 2014.

[22] Der-Chyuan Lou and Chia-Hung Sung, "A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem", IEEE Transactions on Multimedia, vol. 6, no. 3, pp. 501–509, Jun. 2004.

[23] K. Satish, T. Jayakar, Charles Tobin, and K. Madhavi and K. Murali, "Chaos Based Spread Spectrum Image Steganography", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 587–590, May 2004.

[24] Bingwen Feng, Wei Lu, and Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE Transactions on

Information Forensics and Security, vol. 10, no. 2, pp. 243–255, Feb. 2015.

[25] I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image—A new computer art and its application to information hiding", IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 936–945, Sep. 2011.

[26] Ya-Lin Lee and Wen-Hsiang Tsai, "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations", IEEE Transaction on Circuits and Systems for Video Technology, vol. 24, no. 4, pp. 695–703, Apr. 2014.

[27] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 5, pp. 891–899, Sep. 2012.

[28] Ching-Nung Yang, Chih-Cheng Wu, Yi-Chin Lin, and Cheonshik Kim, "Enhanced Matrix-Based Secret Image Sharing Scheme", IEEE Signal Processing Letters, vol. 19, no. 12, pp. 789–792, Dec. 2012.

[29] Subramania Sudharsanan, "Shared Key Encryption of JPEG Color Images", IEEE Transactions on Consumer Electronics, vol. 51, no. 4, pp. 1204–1211, Nov. 2005.