REVERSIBLE DATA HIDING IN ENCRYPTION IMAGE BY USING MAES METHOD

[1]S.Y.Aruna kumara, [2] M.Priyanka,

[1]M-Tech(DECS), Department of Electronics & Communication Engineering, Eluru College of Engineering & Technology, Eluru, AP, India

[2] Assistant professor, Department of Electronics & Communication Engineering, Eluru College of Engineering & Technology, Eluru, AP, India

Abstract

The following paper proposes a novel scheme of data hiding in encrypted images based on lossless compression of encrypted data. In encryption phase, the original content is encrypted into images. As majority of the encrypted data is kept unchanged, the quality of the decrypted image is satisfactory. In the receiver phase, the data is successfully extracted from the image with the help of a public key. The receiver can further recover the original plaintext image without any error. MAES methods, including traditional RDH scheme and unified embedding and scrambling scheme, are adopted to embed watermark in the encrypted image, which can satisfy different needs on image quality and large embedding capacity, respectively

Keywords: Encryption, Decryption, lossless data, VRAE, frame work RRBE.

INTRODUCTION

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption denies the message content to the interceptor. Usually encryption is used when one needs to keep his/her data private. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. Such an algorithm is necessary for the decryption of the message because without it, any party will be able to crack the code and access the data.

Although for a well-designed encryption scheme, large computational resources and skill are required. An authorised recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorised interceptors. The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. There are many transmission media to transfer the data to destination like e-mails; at the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are certain approaches like cryptography and steganography. Let us understand what cryptography and steganography means.

There are existing systems having the key tool for information hiding which is Vacating the room after encryption. It consists of problems such as, the extracted data may contain errors. If there is no availability of sufficient space then some data may be lost & that is why the data is missing at the receiver side which can be termed as data with error. Again the un-availability of memory space is a big problem. Some space is created at the time of data embedding which is a time consuming process. In fig-(1) a

After data extraction the image recovered does not contain the qualities of the original cover. Some distortions are introduced into the image. But it is possible in future that the quality may be improved as compared to existing system.

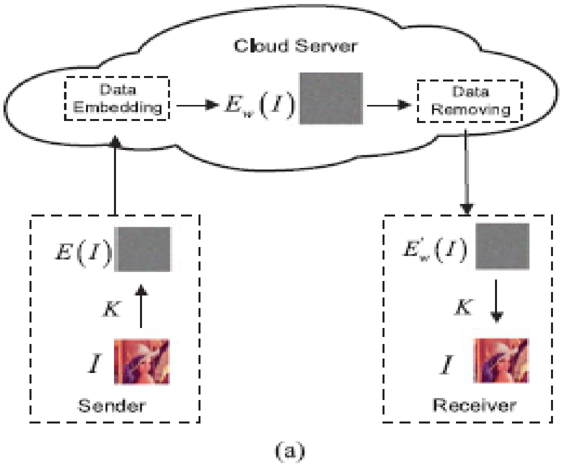


Fig-1(a).Vacating the room after encryption (VRAE)

Previous method

Reversible data hiding techniques:

The quality of the image gets disturbed when the data is embedded into the image. So it is expected that after the data extraction the image quality should be maintained just like the original image. But the image which is obtained contains some distortions. With regards to distortion in image, Kalker and Williams established a rate-distortion copy for RDH, through which they showed the rate-distortion bounds of RDH for without memory covers and proposed a recursive code development which, however, does not move towards the bound .Another promising strategy for RDH is histogram shift (HS), in which the space is saved where data can be embedded by shifting the bins of histogram of gray values at Reserving Room Before Encryption Frame work and RIT based work. In fig-(1) b and c .Reversible data hiding is a technique of RRBE to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible way so that the novel cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy fortification, encryption changes the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption.

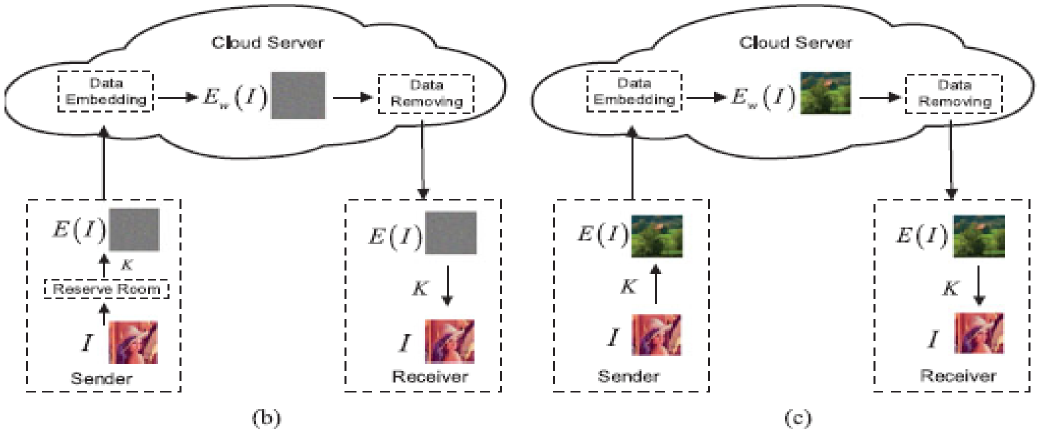


Fig -1(b). Reserving Room Before Encryption Frame work and Fig -1(c).RIT based work

However, in some circumstances that a content owner does not trust the supplier, the ability to influence the encrypted data when maintaining the plain content secret is needed. When the secret data to be broadcasted are encrypted, a supplier without any information of the cryptographic key may compress the encrypted data due to the limited channel resource. Some attempts on RDH in encrypted images have been made. Zhang divided the encrypted image into numerous blocks. By spinning 3 LSBs of the half of pixels in every block, space can be created for the embedded bit.

The data extraction and image recovery proceed by finding which part has been spinned in one block. This process can be grasped with the help of spatial correlation in decrypted image Hong et al. ameliorated Zhang's method at the decryption side by further making use of the spatial correlation using a different estimation equation and side match method to gain much lower error rate. These two methods explained above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction. Zhang et al. recovered the recursive code development for binary covers and proved that this development can gain the rate-distortion bound as long as the compacting algorithm reaches entropy, which launches the correspondence between data compression and RDH for binary covers.

A more popular method is based on difference expansion (DE), in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. So in this way the additional data can be embedded into the covering media which is an improvement to the existing methods

Performance analysis of a reversible data

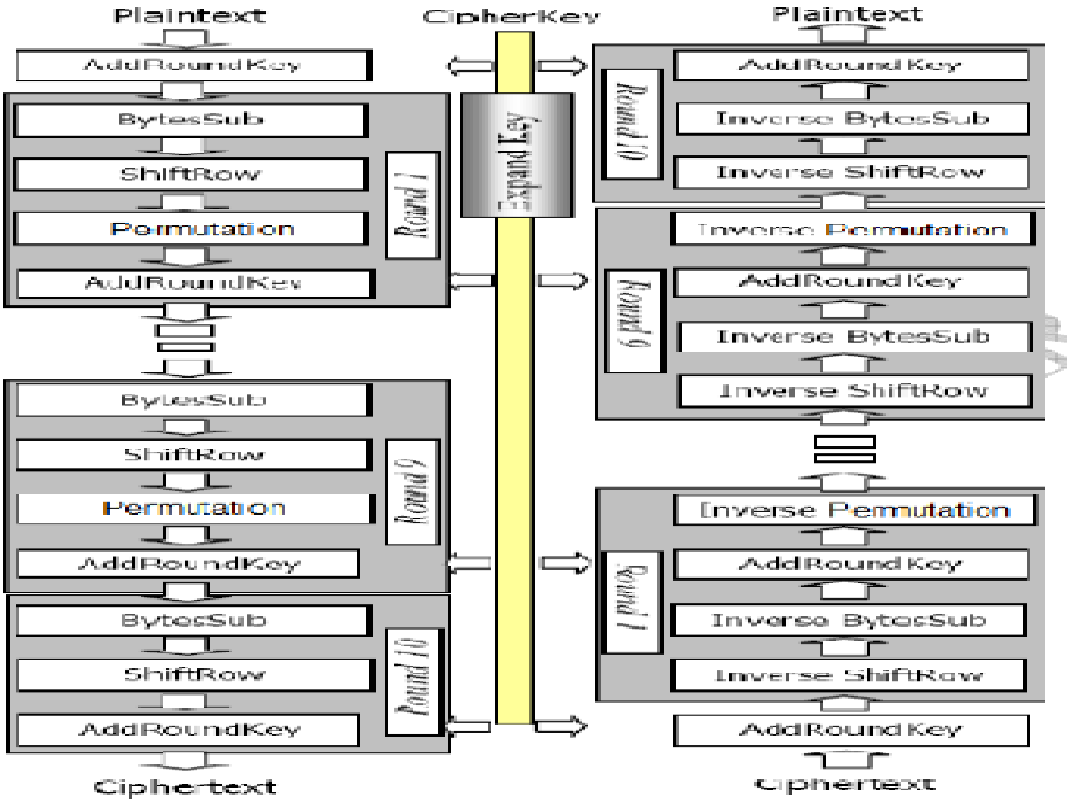
Data embedding in the reversible manner which is the data embedding without any loss embeds the data or payload into digital image in reversible manner. After data embedding the quality of original image may be degraded which is to be avoided. The attractive property of dataembedding in reversible manner is reversibility that is after data extraction the original quality image is restored back. Reversible data embedding hides some information in a digital image in such a way that an approved party could decode the hidden information and also restore the image to its original state.

Proposed method

Modified Advance Encrypted Standard Method

The problem of high calculation and computational overhead, we analyze the Advanced Encryption Standard (AES) and modify it, to reduce the calculation of algorithm and for improving the encryption performance. So we develop and implement a modified AES based Algorithm for all kind of data. The basic aim to modify AES is to provide less computation and better security for data. The modify AES algorithm adjusts to provide better encryption speed. In Modified-AES the block length and the key length are specified according to AES specification: three key length alternatives 128, 192, or 256 bits and block length of 128bits. We assume a key length of 128 bits, which is most commonly implemented. In Modified-AES encryption and decryption process resembles to that of AES, in account of number of rounds, data and key size. The round function consists of four stages. To overcome the problem of high calculation we skip the Mixcolumn step and add the permutation. Mixcolumn gives better security but it takes large calculation that makes the encryption algorithm slow .The other three junctures remain unbothered as it is in Sumira et al : Modified Advanced Encryption Standard For Text And Images123the AES. A single 128-bit block is the input to the encryption and decryption algorithms . This block is a 4×4 square matrix consisting of bytes. This block is copied into the state array.

The state array is modified at each stage of encryption or decryption. Similarly the128-bit key is also depicted into a square matrix. The 128- bit key is expressed into an array of key schedule words: each word is of four bytes. The totals key schedule words for ten rounds are 44 words; each round key is similar to one state. The block diagram of the Modified-AES algorithm with 128 bits data is shown below fig-2(a) and (b)



(a) Encryption (b) Decryption

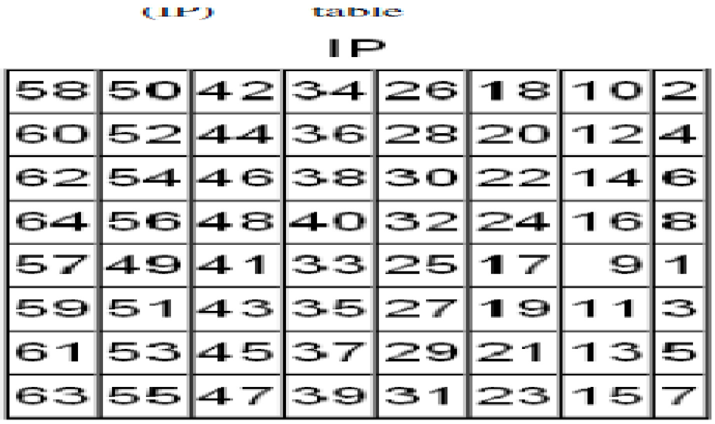
Figure[2]:modified advanced encryption standard

The algorithm is divided into four operational blocks where we observe the data at either bytes or bit levels and the algorithm is designed to treat any combination of data and is flexible for key size of 128 bits. These four operational blocks represent one round of Modified-AES. There are 10 rounds for full encryption.

The four different stages that we use for Modified-AES Algorithm are:

- Substitution bytes
- Shift Rows
- Permutation
- Add Round Key

Substitution Bytes, Shift Rows and Add Round Key remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mixcolumn. These rounds are managed by the following the conversions shown in Fig.1Permutation is widely used in cryptographic algorithms. Permutation operations are interesting and important from both cryptographic and architectural points of view. Tables characterize the permutation and its contrary; the DES algorithm will provide us permutation tables. The inputs to the IP table consist of 64 bits. Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and Shift Rows are also interpreted as 128 bits whereas the Permutation function takes 64 bits. We divide the consequential bits of Shift Rows function into two parts of 64 bits and then take each part of 64 bits as input of permutation tables and shift bits one by one according to that table. We fetch one bit from the source, and put it into the correct position in the destination. Each bit of a block is subject to initial permutation, which can be represented by the following initial permutation



(IP) table

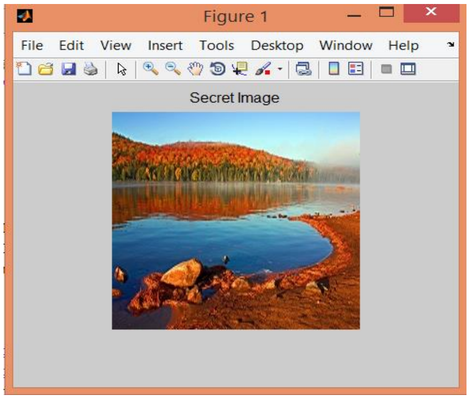
IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

FIG-3

In the permutation table each entry indicates a specific position of a numbered input bit consisting of 64 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 58th bit of the 64-bit block is in first position, the 50th is in second position and so forth. in fig-3

SIMULATION RESULTS



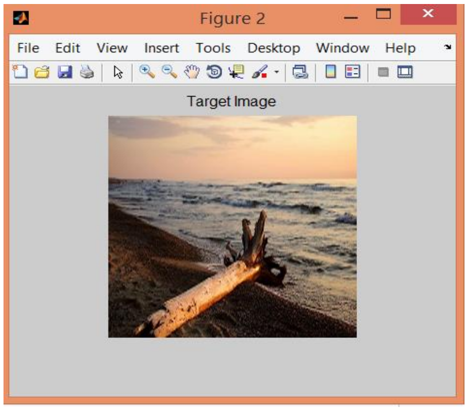


FIG-4 secret image of RIT

FIG-5 Embeddeing of Secret and

Target image

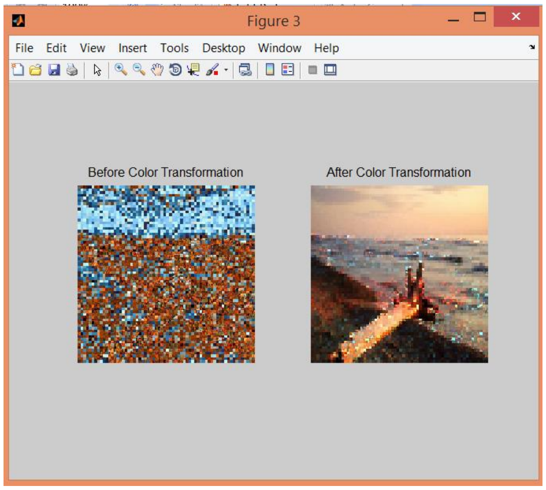


Figure 3
File Edit View Insert Tools Desktop Window Help
Before Color Transformation
After Color Transformation

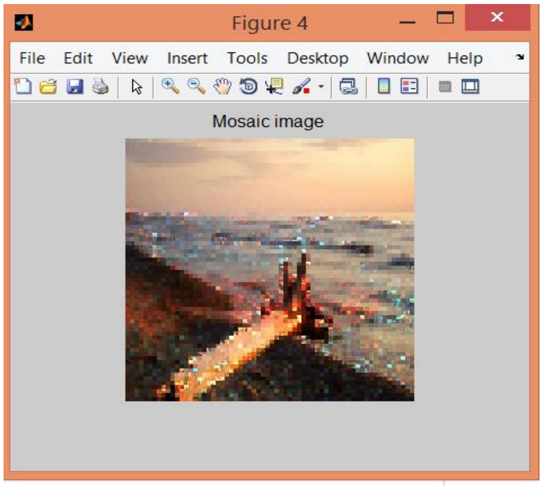
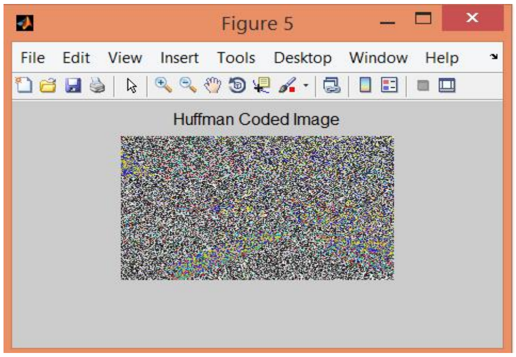


FIG-6 Before Mosaic image transformation

FIG-7 After Mosaic image transformation



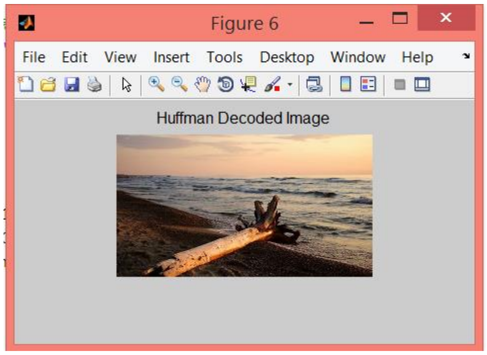
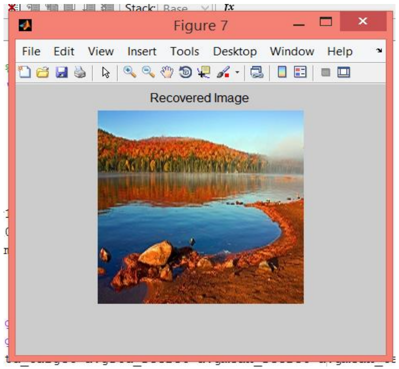


FIG-8 Encoding of Encryption Huffman Code Image

FIG-9Decoding of decryption Huffman Decode Image



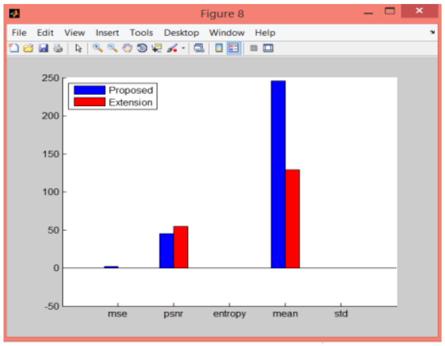


FIG-10 Secret data Recover Image of Proposed method

FIG-11 Previous and Proposed variation levels

CONCLUSION

In this paper we propose a Novel Frame Work for RDH-EI based on MAES. Different from previous frameworks which encrypt a plaintext image into a ciphertext form, RIT-based RDH-EI shifts the semantic of original image to the semantic of another image and thus protect the privacy of the original image. Because the encrypted image has the form of a plaintext image, it will avoid the notation of the curious cloud server and it is free for the cloud sever to choose any one of RDH methods for plaintext images to embed watermark.

We realize an MAES based method by improving the image transformation technique in to be reversible. By MAES, we can transform the original image to an arbitrary selected target image with the same size, and restore the original image from the encrypted image in a lossless way. Two RDH methods including PEE-based RDH and UES are adopted to embed watermark in the encrypted image to satisfy different needs on image quality and embedding capacity. Several interesting problems can be considered in the future, including how to improve the quality of the encrypted image and how to extend idea of MEAS to audio and video.

REFERENCES

[1] K. Hwang and D. Li, “Trusted cloud computing with secure resources and data coloring,” *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.\

[2] F. Bao, R. H. Deng, B. C. Ooi, and Y. Yang, “Tailored reversible watermarking schemes for authentication of electronic clinical atlas,” *IEEE Trans. Inf. Technol. Biomed.*, vol. 9, no. 4, pp. 554–563, Dec. 2005.

[3] F. Willems, D. Maas, and T. Kalker, “Semantic lossless source coding,” in *Proc. 42nd Annu. Allerton Conf. Commun. Control Comput.*, 2004,pp. 1411–1418.

[4] W. Zhang, X. Hu, X. Li, and N. Yu, “Recursive histogram modification:Establishing equivalency between reversible data hiding and lossless data compression,” *IEEE Trans. Image Process.*, vol. 22, no. 7, pp. 2775–2785,Jul. 2013.

[5] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[6] B.ou, X. Li, Y. Zhao, R. Ni, and Y. Shi, “Pairwise prediction-error expansion for efficient reversible data hiding,” *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

[7] I.-C. Dragoi and D. Coltuc, “Local-prediction-based difference expansion reversible watermarking,” *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1779–1790, Apr. 2014.

[8] Z. Ni, Y. Shi, N. Ansari, and S.Wei, “Reversible data hiding,” *IEEE Trans.Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[9] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[10] X. Hu, W. Zhang, X. Li, and N. Yu, “Minimum rate prediction and optimized histograms modification for reversible data hiding,” *IEEE Trans.Inf. Forensics Security*, vol. 10, no. 3, 653–664, Mar. 2015.

[11] X. Hu *et al.*, “Fast estimation of optimal marked-signal distribution for reversible data hiding,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 5, pp. 779–788, May 2013.

[12] W. Zhang, X. Hu, and N. Yu, “Optimal transition probability of reversible data hiding for general distortionmetrics and its applications,” *IEEE Trans. Image Process.*, vol. 24, no. 1, pp. 294–304, Jan. 2015.

[13] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[14] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[15] W. Liu,W. Zeng, L. Dong, andQ.Yao, “Efficient compression of encrypted grayscale images,” *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.