Semiconductor Optoelectronics
ISSN: 1001-5868

IMAGE ENCRYPTION BASED ON WALSH HADAMARD TRANSFORM

Vivek Khalane[1], Shital Mali[2]

[1]Assistant Professor, Department of Instrumentation Engineering, Ramrao Adik Institute of Technology, Navi Mumbai, Maharashtra, India

[2]Assistant Professor, Department of Electronics & electronics Telecommunication Engineering, Ramrao Adik Institute of Technology, Navi Mumbai, Maharashtra, India

Abstract

In this paper, we introduce encryption algorithm have computational complexity, image cryptography application based on Walsh-Hadamard transform. The proposed method consists of image transformation at different level and scrambles the components to design image encryption algorithm. The proposed encryption techniques having unique parameter (key) like order of transform, position of row and column. These unique parameters help to design image encryption algorithm. Original image can be reconstructed when user is known to key parameter. We analyze proposed technique and also represent encryption time for each decomposition level. The results prove that proposed method having high security as compared to state of art methods.

Keywords: Data security, Image encryption, Walsh-Hadamard Transform.

1. Introduction

Signal processing in encrypted domain (SPED) has received attention in recent year. The main motto is to protect user data from unauthorized user. In most of the technologies, data like image, video, text are transfer on large extent across the multimedia and network system [1-5]. In military, medical and various field, it is required to transmit the data which should be secure. To provide such facility, image cryptography plays vital role. Therefore, it is mandatory to design image encryption algorithm to ensure security across various network system. Many researchers designed various encryption techniques. Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT) based algorithm implemented in [6]. Discrete Wavelet Transform in encrypted domain (DWT) is studied and data scrambling method is introduced in [7]. Face verification using quasi homomorphic encryption is executed with intervals [8-9]. New approach is introduced using block cipher by performing nonlinear operations. Chaos technique implemented by selecting confusion and diffusion in many rounds. Lossless and reversible data hiding process is introduces in encryption domain [10-15]. Walsh Hadamard Technique (WHT) is widely used in signal processing for various application such as image compression [16], coding [17], communication and filtering [18]. Main feature of WHT is that calculation doesn't involve division and multiplication, WHT is used in video compression i.e. H.264/MPEG-4 AVC format and VP9 [19]. The quality of

encryption algorithm is decided by complexity of mathematical calculation. WHT method is widely used in signal processing for various application like bioinformatics, multimedia data, filtering, and array analysis. Many times, attacker can retrieve data by manipulating system algorithm [20-22]. To address this problem, we have scrambled the order of key parameters. By decomposing input image and shuffling the parameters, we can secure the image. This paper represents the new encryption method using WHT [23]. Key parameters are arranged as stack format in Bookkeeping vector which consist of number of decomposition components, decomposition technique and the order of key parameters. The encryption algorithm can be designed by selecting appropriate parameters. This paper is organized as follows: Review of Walsh Hadamard Transform briefly explained in section II. Image encryption technique is proposed in section III. Section IV brief about experiment using WHT and result discussion and conclusion in section V.

2. PREVIEW OF WALSH HADAMARD TRANSFORM

The WHT consist of natural ordering, dyadic ordering and sequence ordering, let we define parameter like

$$H_1 = [1] \text{ and } H_2 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{bmatrix}$$

Recursive matrix of WHT is starting from H2. In proposed method, we exclude the scale vector in H2 for simplification to apply WHT in encrypted domain [24].

1) Hadamard Ordering: $H_{h,M}$ of size $M \times M$ Hadamard transform obtained using recursive relation:

$$H_{h,M} = H_2 \otimes H_{h,M/2} = \begin{bmatrix} H_{h,2^{\vartheta-1}} & H_{h,2^{\vartheta-1}} \\ H_{h,2^{\vartheta-1}} & -H_{h,2^{\vartheta-1}} \end{bmatrix} \qquad (1)$$

Where, $\vartheta = \log_2 M$, $\vartheta = 1, 2, 3 \cdots$ and $\otimes$ is Kronecker product operator

2) Paley Ordering: Paley ordered transform matrices can be given as:

$$H_{p,M} = (H_2 \otimes H_{p,M/2}) P_{2,M/2}^T \qquad (2)$$

Where, $P_{2,M/2}$ is a perfect shuf e matrix and $(\cdot)^T$ is the matrix transposition operator.

3) Walsh Ordering: The Walsh ordered WHT is widely used in signal processing theory. Walsh ordering transform is given by:

$$H_{\omega,M} = \left(H_2 \otimes H_{\omega,M/2}\right) P_{2,M/2}^T \left(E_{M/4} \otimes \begin{bmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{bmatrix} \right) \qquad (3)$$

Where, E_M is identity matrix of size $M \times M$

Definition of two dimensional WHT is given by:

$$\overset{\cup}{V}(m,n)=\frac{1}{M}\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}H_g(m,i)X(i,j)H_g(j,n),m,n=0,1,...,M-1 \qquad (4)$$

Where, X is input image of size $M \times M$.

3. Design Methodology: Image Encryption Based on Walsh Hadamard Transform

In this section, we propose image encryption using WHT technique. We decompose input image using Walsh Hadamard technique.

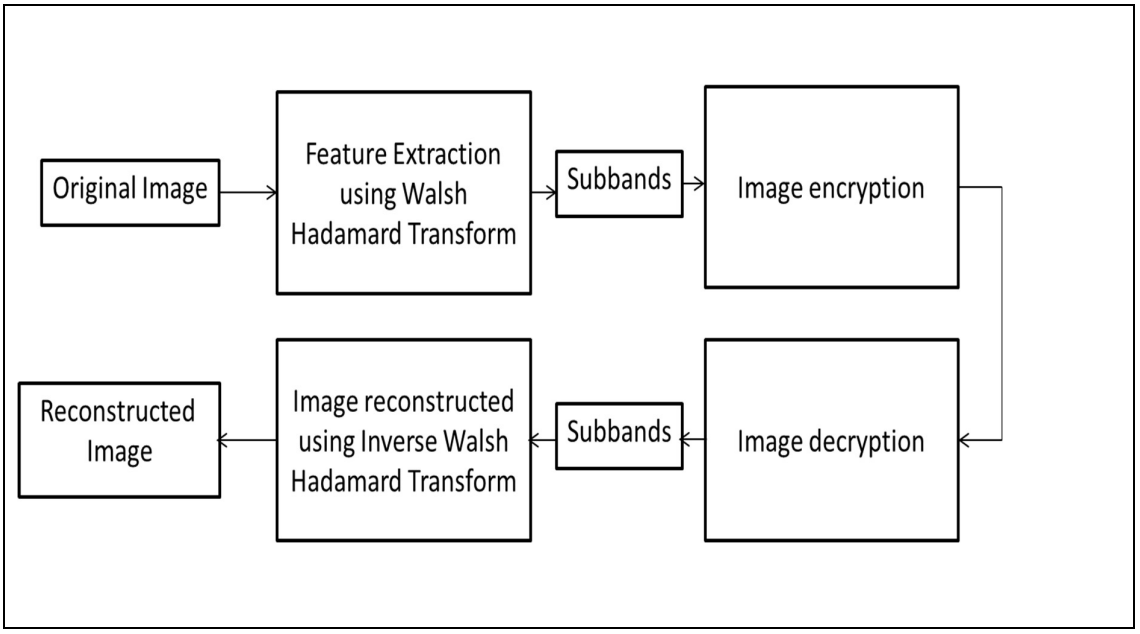

Fig.1. Image Encryption

Walsh Hadamard Transform is adapted for various application such as image compression, image transform coding, image watermarking. The proposed method is explained in Fig. 1. In this method, features of input image size M * N are extracted using WHT. Proposed transform is applied to input image at particular order and row/column of transformed image is scrambled in random manner. The key parameters after transformation i.e. order WHT and positioning of rows and columns is used for image encryption. Original image is reconstructed using inverse WHT. In proposed method, order of Walsh Hadamard transform and positioning of row/column of transformed image act as key parameters. Key parameters like order of Walsh Hadamard transform and positioning of row/column of transformed image are arranged in stack format which is very unique and known to user only. Anybody can decrypt the original image only when user known key parameters.

4. Experimentation and Result

For experimentation purpose, we have applied encryption method on standard images with

size of 256 × 256 like Cameraman, Peppers, Lena, Barbara, Baboon images as shown in Fig. 2(i)-(v). We used MATLAB with system memory 4GB and Intel core 3 processor. Walsh Hadamard Transform coefficient and reconstructed image is shown in in Fig. 2(vi)-(x) and 2(xi)-(xv). Correlation between original and reconstructed image determine the quality of encryption method [25]. Correlation coefficient for various images is given in Table 1.

Table1. Proposed correlation coefficient of image

Image	Correlation
Cameraman	0.0690
Peppers	0.0773
Lena	0.0594
Barbara	0.0640
Baboon	0.0522

The encryption time for each decomposition level is tabulated in Table 2.

Table.2. Encryption time for decomposition level

Decomposition level	Speed of encryption in second
I	0.0235
II	0.01345
III	0.01744
IV	0.01824
V	0.01984

The effectiveness algorithm is proved by comparing with the proposed algorithm with the state of art techniques. Correlation coefficient of Lena image using proposed design is compared with existing methods like parameterized halfband filterbank (PHFB) approach [08], discrete wavelet transform (DWT) [23], Fresnel transform [26] shown in Table 3. It is observed that proposed algorithm has less correlation as compared latest methods which ensure more security.

Table.3 Comparison with latest algorithms

Method	Correlation Coefficient
PHFBs [08]	0.07235
DWT [23]	0.09813
Fresnel Transform [26]	0.0821
Proposed Method	0.0594

5. CONCLUSION

This paper introduces new technique of image encryption based on Walsh Hadamard

transform. Order of Walsh Hadamard transforms and positioning of row/column of transformed image act as key parameters. Proposed algorithm has less correlation coefficient between input and encrypted image as compared with latest method. It has been ensured that proposed algorithm offer high security which difficult to crack.

References:

1. M. Kurt Pehlivanoğlu and N. Duru, "Encryption of Walsh Hadamard Transform applied images with the AES encryption algorithm," 2016 24th Signal Processing and Communication Application Conference (SIU), Zonguldak, 2016, pp. 301-304, doi: 10.1109/SIU.2016.7495737.
2. Sneha, P.S., Sankar, S. & Kumar, A.S. A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps. J Ambient Intell Human Comput 11, 1289–1308 (2020).
3. Zheng P., Huang J. (2013) Walsh-Hadamard Transform in the Homomorphic Encrypted Domain and Its Application in Image Watermarking. In: Kirchner M., Ghosal D. (eds) Information Hiding. IH 2012. Lecture Notes in Computer Science, vol 7692. Springer, Berlin, Heidelberg.
4. Zheng P, Huang J. Efficient Encrypted Images Filtering and Transform Coding with Walsh-Hadamard Transform and Parallelization. IEEE Trans Image Process. 2018 Feb 5. doi: 10.1109/TIP.2018.2802199. Epub ahead of print. PMID: 29994419.
5. Khanam, T.; Dhar, P.K.; Kowsar, S.; Kim, J.-M. SVD-Based Image Watermarking Using the Fast Walsh-Hadamard Transform, Key Mapping, and Coefficient Ordering for Ownership Protection. Symmetry 2020, 12, 52.
6. Khurana, Mehak and H. Singh. “Asymmetric optical image encryption using random Hilbert mask based on fast walsh hadamard transform.” 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN) (2017): 374-377.
7. V S & A. T. Discrete Walsh Hadamard transform based visible watermarking technique for digital color images. International Conference on Graphic and Image Processing (ICGIP 2011). 2011. Available from: 10.1117/12.913308.
8. Q. Yi, L. Heng, L. Liang, Z. Guangcan, C. Siong, and Z. Guangya, "Hadamard transform-based hyperspectral imaging using a single-pixel detector," Opt. Express 28, 16126-16139 (2020).
9. Tu, H., Bu, W., Wang, W. et al. Applicability of Hadamard relaxation method to MMW and THz Imaging with compressive sensing. SIViP 11, 399–406 (2017).
10. V. P. Khalane and U. S. Bhadade, “A parameterized halfband filterbank design for image encryption,” in 2018 IEEE 13th International Confer- ence on Industrial and Information Systems (ICIIS), pp. 32–35, IEEE, 2018.
11. V. P. Khalane and U. Bhadade, “Image encryption using wavelet transform over finite field,” in Proceedings of the 10th International Conference on Security of Information and Networks, pp. 257–261, ACM, 2017.
12. Wang, Li, and Yan Feng. "Compressed sensing of hyperspectral images based on scrambled block Hadamard ensemble." Journal of Electronic Imaging 25, no. 6 (2016): 063021.
13. Luo, Yu-Ling, Rong-Long Zhou, Jun-Xiu Liu, Sen-Hui Qiu, and Yi Cao. "A novel image encryption scheme based on Kepler’s third law and random Hadamard transform." Chinese

Physics B 26, no. 12 (2017): 120504.
14. B. Patil, G. Sharma, P. Patwardhan, and V. Gadre, “A generalized approach for finite precision 5/3 filter design,” in In the Proceedings of National conference on Communications NCC 2007, pp. 112–115, 2007.
15. Sui, Liansheng, and Bo Gao. "Color image encryption based on gyrator transform and Arnold transform." Optics & Laser Technology 48 (2013): 530-538.
16. Drago, Nicolò, and Christian Gérard. "On the adiabatic limit of Hadamard states." Letters in Mathematical Physics 107, no. 8 (2017): 1409-1438.
17. Sang, Jun, Hongling Luo, Jun Zhao, Mohammad S. Alam, and Bin Cai. "Image encryption with chaotic map and Arnold transform in the Gyrator transform domains." In Pattern Recognition and Tracking XXVIII, vol. 10203, p. 102030P. International Society for Optics and Photonics, 2017.
18. P. P. Vaidyanathan, Multirate Systems and Filter banks. NJ: Englewood Cliffs Prentice-Hall, 1993
19. Vadhi, Radhika, Veera Swamy Kilari, and Srinivas Kumar Samayamantula. "Image Fusion Algorithms Using Human Visual System in Transform Domain." In IOP Conference Series: Materials Science and Engineering, vol. 225, no. 1, p. 012156. IOP Publishing, 2017.
20. Chan, Kimberly L., Nicolaas AJ Puts, Michael Schär, Peter B. Barker, and Richard AE Edden. "HERMES: Hadamard encoding and reconstruction of MEGA-edited spectroscopy." Magnetic resonance in medicine 76, no. 1 (2016): 11-19.
21. Zhu, Bo, Jeremiah Z. Liu, Stephen F. Cauley, Bruce R. Rosen, and Matthew S. Rosen. "Image reconstruction by domain-transform manifold learning." Nature 555, no. 7697 (2018): 487-492.
22. [22] Kumar, Ravi, Basanta Bhaduri, and Bryan Hennelly. "QR code-based non-linear image encryption using Shearlet transform and spiral phase transform." Journal of Modern Optics 65, no. 3 (2018): 321-330.
23. [23] D. Goswami, N. Rahman, J. Biswas, A. Koul, R. L. Tamang, and Bhattacharjee, “A discrete wavelet transform based cryptographic algorithm,” IJCSNS, vol. 11, no. 4, p. 178, 2011. Stand. Abbrev., in press.
24. [24] Corcoran, Timothy C. "Compressive detection of highly overlapped spectra using walsh–hadamard-based filter functions." Applied spectroscopy 72, no. 3 (2018): 392-403.
25. [25] Kolouri, Soheil, Se Rim Park, and Gustavo K. Rohde. "The radon cumulative distribution transform and its application to image classification." IEEE transactions on image processing 25, no. 2 (2015): 920-934.
26. [26] Luan, Guangyu, et al. "Asymmetric image encryption and authentication based on equal modulus decomposition in the Fresnel transform domain." IEEE Photonics Journal 11.1 (2018): 1-7.