Biomedical Research 2018; Special Issue: S145-S149

ISSN 0970-938X
www.biomedres.info

A novel privacy preserving visual cryptography based scheme for telemedicine applications.

Hare Ram Sah[1]*, G. Gunasekaran[2], Latha Parthiban[3]

[1]Faculty of Computer Science and Engineering, Sathyabama University, Chennai, India

[2]Department of Computer Science and Engineering, Meenakshi College of Engineering, Chennai, India

[3]Department of Computer Science, Pondicherry University CC, Pondicherry, India

Abstract

With huge quantity of patient's medical images to be shared between specialists and clinics for improving medical diagnosis, need for privacy protection of patient details has increased. To achieve this, care must be taken that during reception, image quality must be preserved and retrieved image should be error free. In this paper, a unique concept of tiling has been used on image patterns using visual cryptography to achieve privacy preservation. The medical image is partitioned into frames using the concept of rhombus and in the deformed image tiles are formed within the different partitions, which are transmitted along with encrypted stegano-tiles. The reconstruction of original image is obtained by stacking the tiles and this error free methods performance is tested using multi scale structural similarity index and CUDA enabled GPUs.

Keywords: Visual cryptography, Tiling, Rhombus, Telemedicine.

Accepted on July 28, 2017

Introduction

A tiling can be periodic or non-periodic and periodic is one in which image can outline a region that tiles the plane by translation that is, by shifting the position of the region without rotating or reflecting it. Original image and the tiled image are in the same size. Hwang proposed the efficient watermark method based on Visual Cryptography (VC) and the watermark pattern can be retrieved without any information about original image [1]. Qi proposed a method to recover the secret image which is lossless [2]. Soman et al. proposed two XOR-based VC algorithms, *viz*., XOR-based VC for general access structure and adaptive region incrementing method [3]. Ananth et al. proposed research design that implements a barcode encoder based steganography method [4]. Linju et al. proposed the sealing algorithm where two secret images are sent at the same time by converting them to halftone representations [5]. Deepika et al. proposed a scheme to share a secret among 'n' participants, i.e. an 'n' out of 'n' secret sharing scheme, based on a new number system called Permutation Ordered Binary (POB) number system and Chinese Remainder Theorem (CRT) [6]. Niimi et al. proposed a method for preserving privacy in electronic health record [7]. Parallel cryptosystem is introduced, using which all subtiles are transmitted at the same time and in, an algorithm to for encryption of secret images into meaningful images is proposed [8,9].

Proposed Methodology

The proposed privacy preserving method is achieved by partitioning the medical image by tiling, applying stegano algorithm followed by simple encryption which is decrypted in receiving end as shown in Figure 1.

Partitioning the medical image by tiling

Tiling is a way of arranging identical plane shapes, so that they completely cover an area without overlapping. The rhombus based partition is placed over the secret image. The secret image is divided into six subsets based on the angles used in Figure 2 and partitioned as shown in Figure 3.

Applying stegano algorithm to generate stegano tiles

The steps for stegano algorithm are given by:

- Introduce lamps in secret figure.
- Label the edges of the subsets as H_{ik}, i=1 to L (number of subsets) and k=1 to number of edges in ith tile.
- The connecting among subsets specified in the stegano tile.

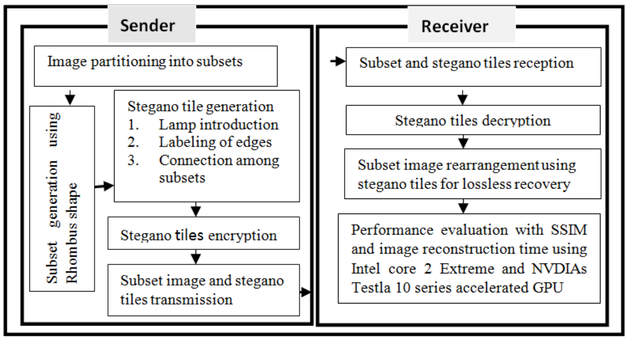

Sender
Image partitioning into subsets
Subset generation using Rhombus shape
Stegano tile generation
1. Lamp introduction
2. Labeling of edges
3. Connection among subsets
Stegano tiles encryption
Subset image and stegano tiles transmission
Receiver
Subset and stegano tiles reception
Stegano tiles decryption
Subset image rearrangement using stegano tiles for lossless recovery
Performance evaluation with SSIM and image reconstruction time using Intel core 2 Extreme and NVDIAs Testla 10 series accelerated GPU

Figure 1. Proposed methodology.

Lamps are introduced to rhombus shape and the generated five lamps and labelling process are shown in Figure 4. The generated stegano tile is shown in Figure 5.

Encryption of stegano tile

The encryption is based on the attribute of database and if the data type of attribute is text, then it is encrypted into numerical value and if the data type of attribute is numeric, then it is encrypted into text as in Table 1.

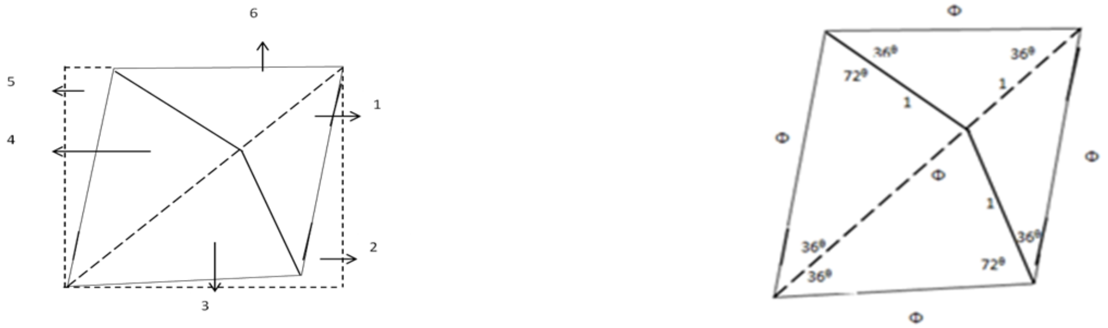


Figure 2. Rhombus and its application to the secret image.

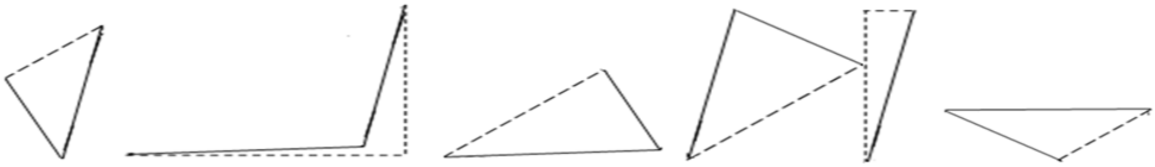


Figure 3. Partitioned subset (listed from 1 to 6 in order).

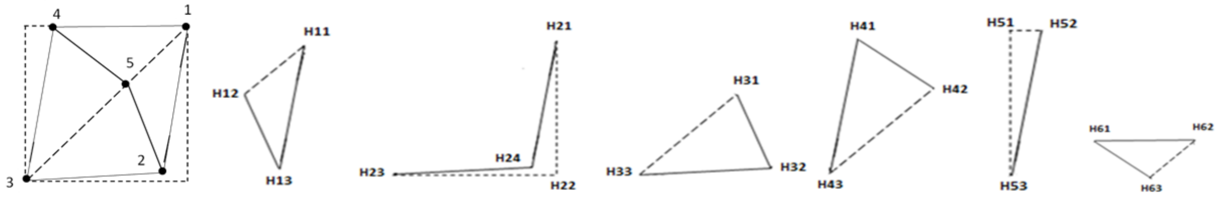
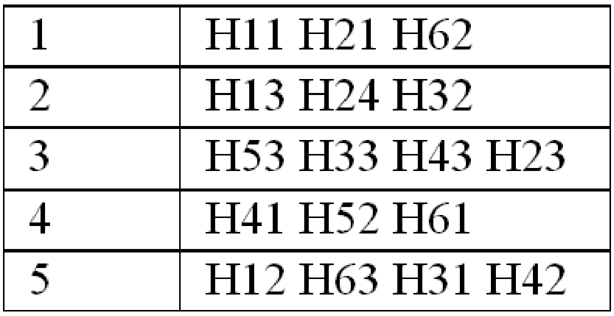


Figure 4. Lamps and labelled tiles.

Table 1. Encryption of text and numeric attribute.

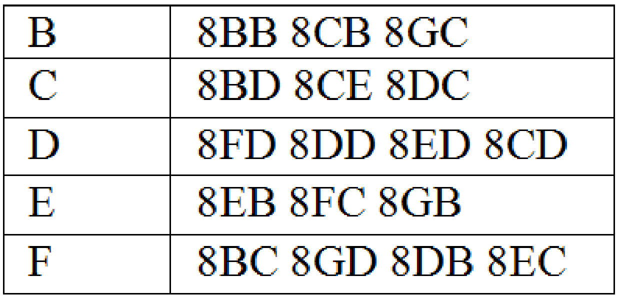
Text attribute	Key	Text attribute	Key	Text attribute	Key	Text attribute	Key	Text/Numeric attribute	Key	Numeric attribute	Key
A	1	G	7	M	13	S	19	Y	25	4	E
B	2	H	8	N	14	T	20	Z	26	5	F
C	3	I	9	O	15	U	21	0	A	6	G
D	4	J	10	P	16	V	22	1	B	7	H
E	5	K	11	Q	17	W	23	2	C	8	I

F	6	L	12	R	18	X	24	3	D	9	J



1	H11 H21 H62
2	H13 H24 H32
3	H53 H33 H43 H23
4	H41 H52 H61
5	H12 H63 H31 H42

Figure 5. Generated stegano tile.



B	8BB 8CB 8GC
C	8BD 8CE 8DC
D	8FD 8DD 8ED 8CD
E	8EB 8FC 8GB
F	8BC 8GD 8DB 8EC

Figure 6. Encrypted stegano tile.

The attribute based encryption technique is applied to the Figure 6 and the encrypted stegano tile is shown in Figure 6. This encrypted stegano tile along with labelled tiles are received in the receiving end which is decrypted (same as Figure 5) and help in the reconstruction of the original image.

Results and Discussions

The proposed algorithm is tested on the CT image (Figure 7) which is partitioned based on the procedure in Figure 3.

The generated tiles are labelled based on rhombus shape as shown in Figure 8 which is then encrypted (Figure 6) and transmitted. The received stegano tile in encrypted form is shown in Figure 9 and decrypted stegano tile is shown in Figure 10. In reconstruction process (Figures 11a and 11b), the lablled tiles are joined in step by step manner from decrypted stegano tile (Figure 6) to obtain the secret image.

The proposed algorithm was tested on the 4 CT medical images (obtained from www.aylward.org/notes/open-access-medical-image-repositories) and the reconstructed images are compared with original images in terms of Multi-scale Structural Similarity Index (SSIM). Table 2 shows the SSIM obtained for the 4 test images.

The proposed method is not dependent on the order of arrival of tiles like the conventional method as in Figure 12 (a). NVIDIA's Tesla GPUs reconstruction time performance of the partitioned subsets using encrypted stegano tile was found to be only 72 seconds against 368 seconds taken by Intel's core 2 Extreme as shown in Figure 12 (b).

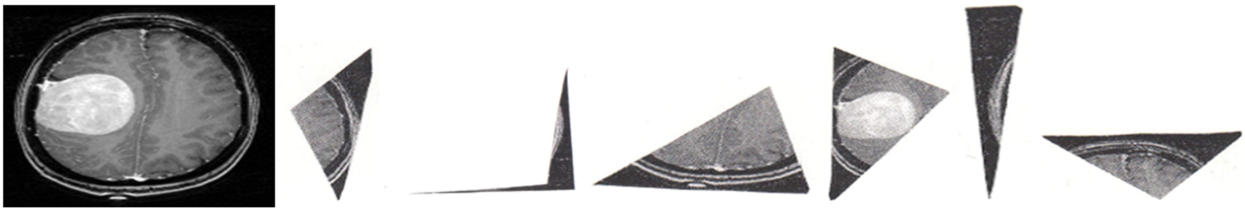


Figure 7. Secret medical image and its partitioned subsets.

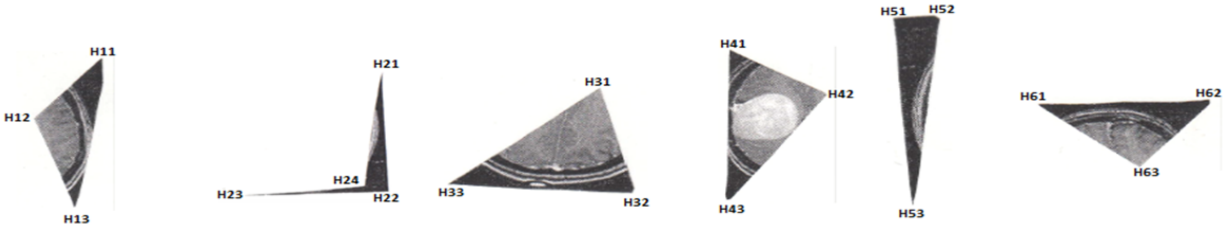
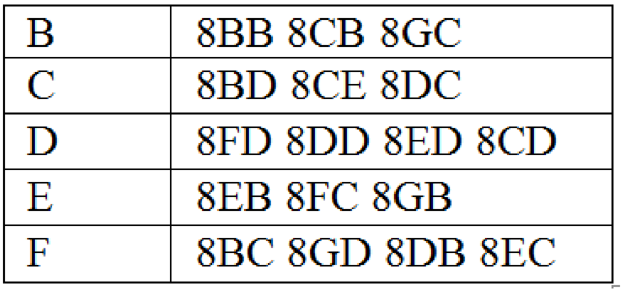
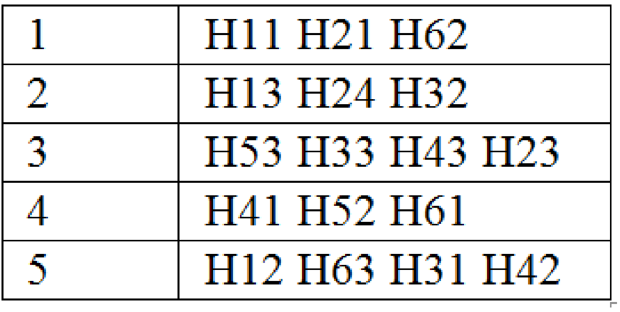


Figure 8. Labelled tiles of medical image.



B	8BB 8CB 8GC
C	8BD 8CE 8DC
D	8FD 8DD 8ED 8CD
E	8EB 8FC 8GB
F	8BC 8GD 8DB 8EC

Figure 9. Received stegano tile.



1	H11 H21 H62
2	H13 H24 H32
3	H53 H33 H43 H23
4	H41 H52 H61
5	H12 H63 H31 H42

Figure 10. Decrypted stegano tile.

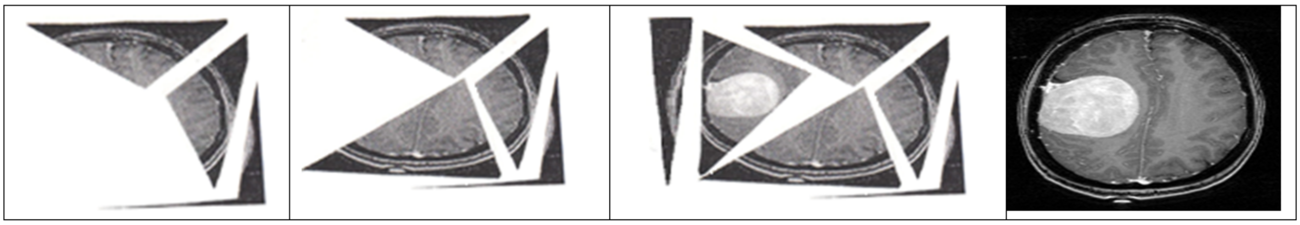


Figure 11a. Procedure for reconstruction of transmitted medical image in receiving end.

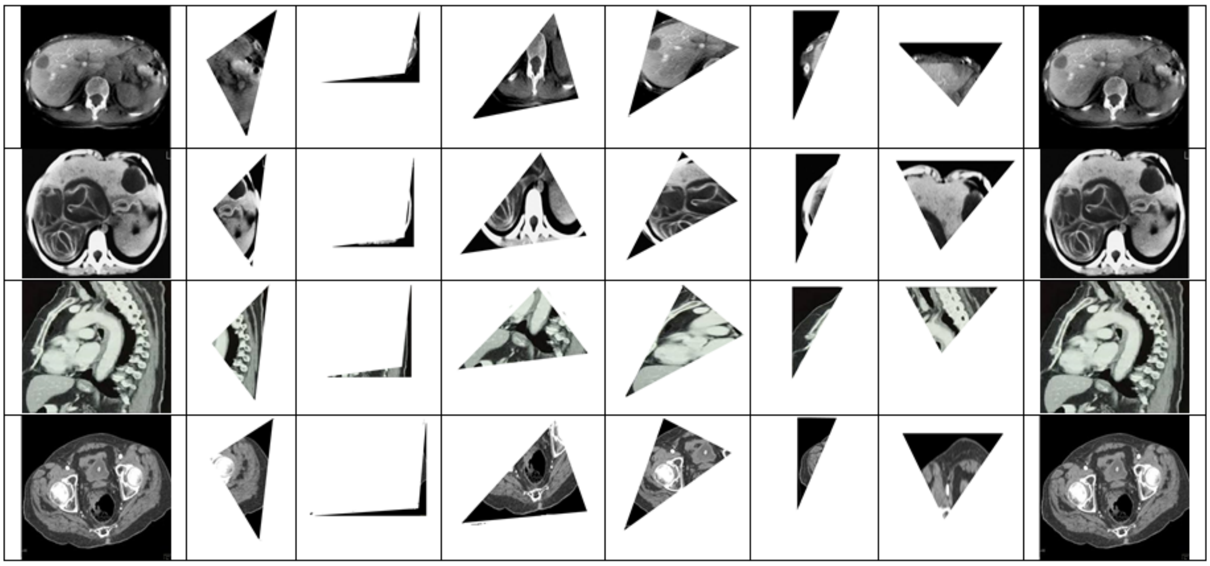


Figure 11b. Test images, partitioned subsets and image reconstruction from subsets.

Table 2. SSIM results for the test images.

Test Image	SSIM
1	0.9878
2	0.9912
3	0.9868
4	0.9976

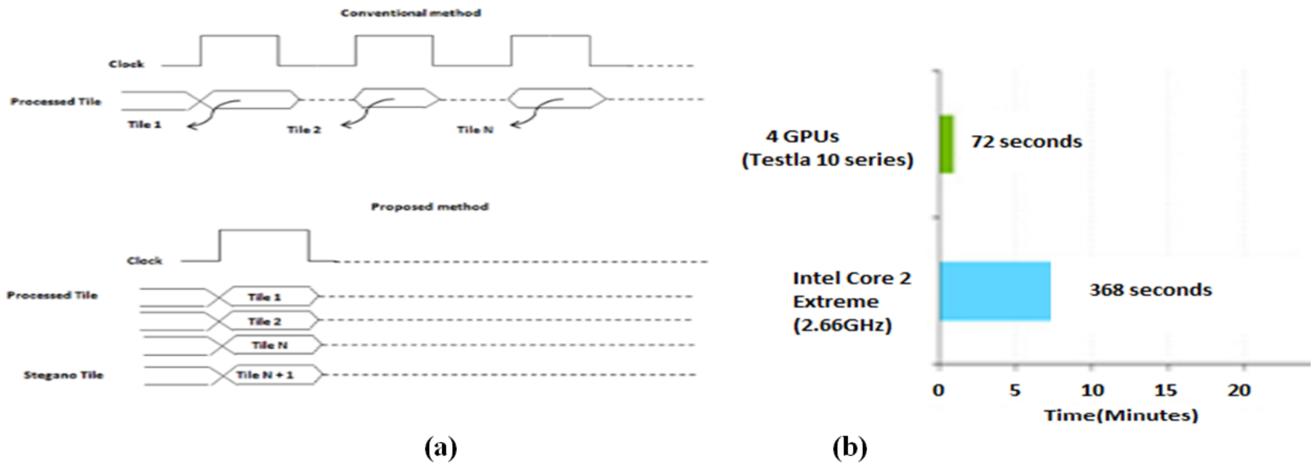


***Figure** 12. (a) Transmission clock cycle; (b) Reconstruction time.*

Conclusions

In this paper as reconstruction of original medical image is done by stacking the stegano tiles, it is an enhanced privacy preserving lossless technique for e-health applications. The method is easy to implement and does not need complicated cryptographic computations. The received images are found to have multi scale structural similarity nearing 1. The reconstruction time was also found to be very less when CUDA enabled GPUs were used. Future work is to concentrate on other efficient tiling shapes and use other Testla processors for faster reconstruction time.

Acknowledgement

The authors would like to thank Pondicherry University for allowing access to CUDA enabled GPU computing facility for the research work.

References

1. Ren-Junn H. A digital image copyright protection scheme based on visual cryptography. Tamkang J Sci Eng 2000; 3: 97-106.
2. Xin Q. Lossless recovery of multiple decryption capability and progressive visual secret sharing. Int J Grid Dist Comp 2016; 9: 51-60.
3. Nidhin S, Smruthy B. XOR-based visual cryptography. Int J Cybernet Inform 2016; 5: 253-264.
4. Vijay AS, Sudhakar P. Performance analysis of a combined cryptographic and steganographic method over thermal images using barcode encoder. Indian J Sci Technol 2016; 9: 1-5.
5. Linju PS, Sophiya M. An efficient interception mechanism against cheating in visual cryptography with non-pixel expansion of images. Int J Sci Technol Res 2016; 5: 102-106.
6. Deepika MP, Sreekumar A. A novel secret sharing scheme using POB number system and CRT. Int J Appl Eng Res 2016; 11: 2049-2054.
7. Niimi, Yukari O, Katsumasa. Examination of an electronic patient record display method to protect patient information privacy. CIN: Comp Inform Nurs 2017; 35: 100-108.
8. Hong-Mei Y, Ye L, Tao L, Ting H, Li-Hua G. A new parallel image cryptosystem based on 5D hyper-chaotic system. Signal Processing: Image Commun 2017; 52: 87-96.
9. Kanso A, Ghebleh M. An algorithm for encryption of secret images into meaningful images. Optics Lasers Eng 2017; 90: 196-208.

*Correspondence to

Hare Ram Sah

Faculty of Computer Science and Engineering

Sathyabama University

Chennai

India