International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

PPDM for Medical Data using Visual Cryptography

Subhashree.P, G.Gunasekaran

Abstract: Privacy preserving data mining is a growing field with advancements reported frequently. In this paper, for maintaining privacy of medical data of patients, a novel visual crypto technique of peeling with modular scheme is proposed. In this work, using the concept of group theory, PPDM for medical data is done using Verilog.

***Keywords** : Visual Cryptography,Concurrency, Image Slicing, privacy preservation.*

I. INTRODUCTION

An algorithm in data mining deals with creating a suitable model that maps the input and output attributes appropriately. Using the data provided, the algorithm creates patterns depending on the iterations thereby finding parameters for the model to be created. These created model is further optimized using all the input data which is applied on it . Data-mining algorithms which is the core of the data-mining process provide knowledge based decision-making capabilities for many operations in data mining. The algorithm creates a model from the input data which can be clustered and classified for better accuracy.

Privacy Preservation Data Mining (PPDM) is very important for medical data as the identity of persons having specific disease must be kept secure. Many techniques are proposed in literature and the paper is organized as follows: section 2 deals with literature survey, section 3 with proposed algorithm, section 4 with experimental results and section 5 ends with conclusions and future work.

II. LITERATURE SURVEY

Private data are used for research purpose but anonymization has to be maintained to limit the disclosure risks. Privacy preservation in data mining has become an important research area with many literature surveys. In [1-5] the authors describes various proposed methods in visual cryptography. In [6-9], various data mining techniques with privacy preservation is discussed along with various privacy disclosure problems.

III. PROPOSED ALGORITHM

The three processes done in this work is as follows:

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Mrs.Subhashree.P*, Research Scholar, Sathyabama Institute of Science and Technology.
Dr. G.Gunasekaran, Principal, J.N.N Institute of Engineering.

1. The messages must be represented in the range between 0 and (n-1).
2. Create cipher text by encryption.

Decrypt the cipher text.

The four rounds involved for encryption are as follows:

1. Frames formation: Frames are formed by subdividing the images.
2. Frame Slicing: In this step, the frames are further divided into number of slices.
3. Randomization of the slice positions: In this step four bytes in each column are taken as input and generated as output.
4. Exploiting Concurrency with hardware: In this process the slices are processing concurrently in multiple partitions.

The steps involved in decryption are as follows:

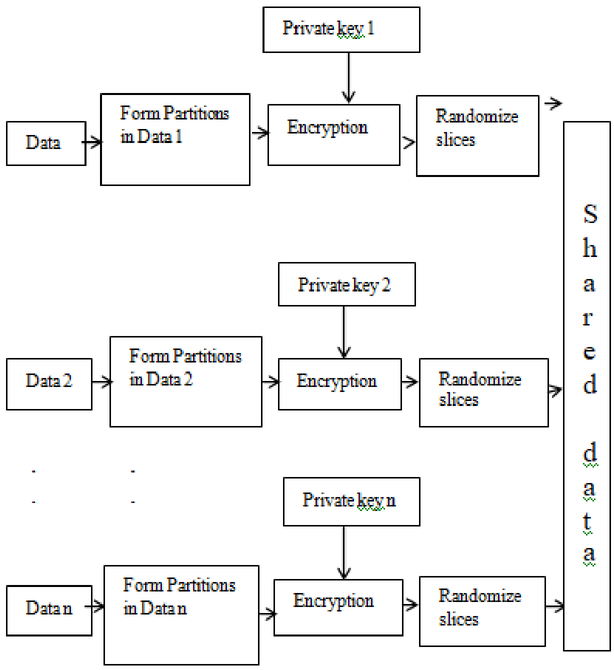
1. Reverse shift slice positions
2. Combine frames
3. Reconstruct image

The entire process of PPDM using visual cryptography is shown in figure 1.

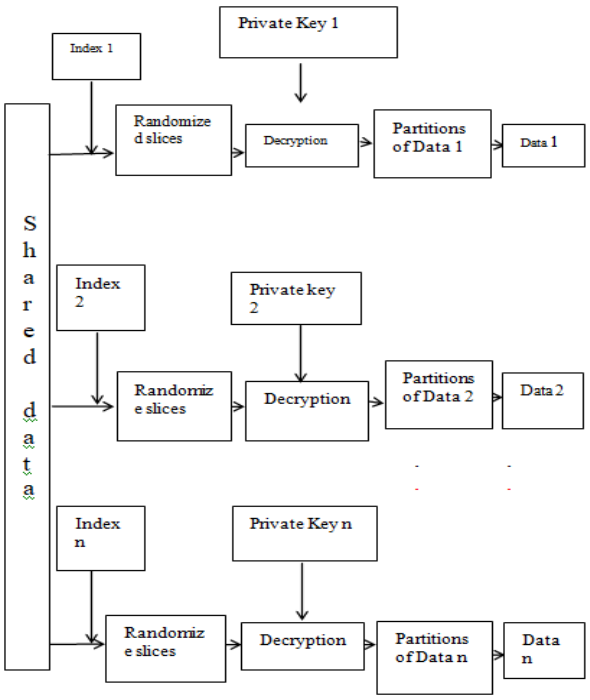
For assigning different levels of slicing, the randomized slice positions for eight slices are shown in Table I.

Table 1: First level slices

7	2	4	6	5	3	1	8



(a)Encryption



(b)Decryption

Figure 1 Privacy preserving data mining using visual cryptography with concurrent slice tracking. From Table I, it can be seen that image sub-frame of M x M of total size N x N is divided into eight frames. The split slices of a sub-frame are rearranged randomly in Table-I [i.e.1st position is occupied by 7th slice, 3rd position is occupied by 4th partitioned slice and so on]. Using Table-I and the positional information, the destegano operation is performed. The recovered slice are shown in Table 2.

Table 2: Recovered slices

1	2	3	4	5	6	7	8

Slice position tracking algorithm is shown below.

```
Initialize array1,array2;p=j=1;/*p& j are array indices */
   Start:
   if array1 [p] ==j;
    {
      array2 [j] =p; j=j+1; p=1;
   }
   else p=p+1;
```

The procedure of destegano algorithm is implemented using image of size N x N, is taken which is sliced as in figure 2.

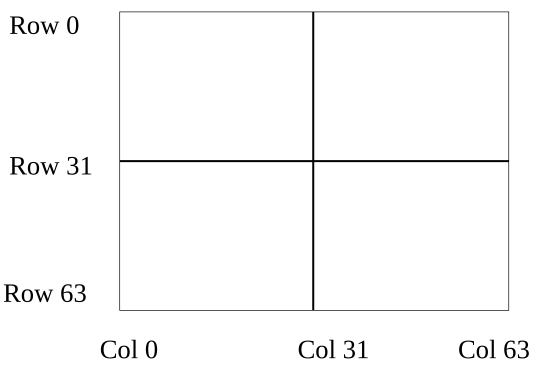


Figure 2 N x N image with four partitions

For p=3; the 3rd slice in 1st partition will be of size $M_{31}{}^{(1)}$ = Row 0 to Row 31 and $M_{32}{}^{(1)}$ =Col 8 to Col 11 and so on as shown in figure 3.

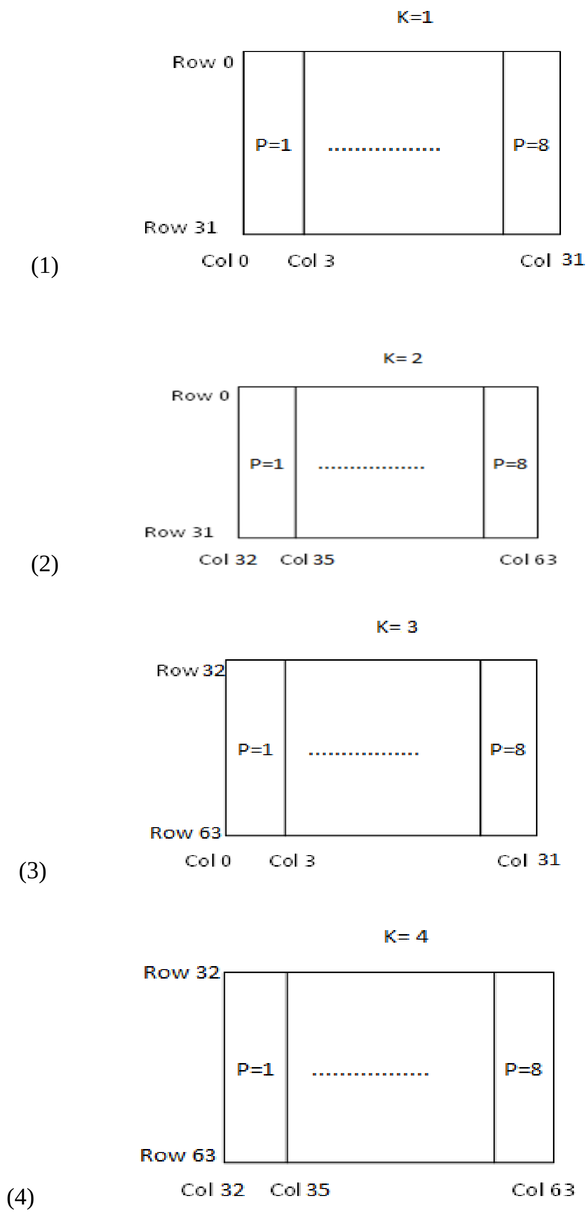


Figure 3 Partitions and slices

For concurrent processing, the sequential search is done as shown in figure 4.

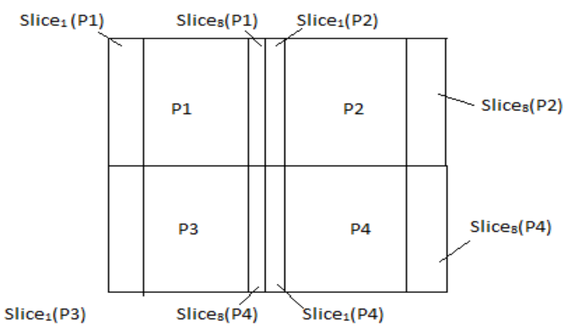


Figure 4 sequential search

The timing and task handled relation is given in Table 3.

Retrieval Number: B3012129219/2019©BEIESP
DOI: 10.35940/ijeat.B3012.129219
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table 3 : Time and task handled relation

Time	Tasks handled
t_1	$Slice_1^{(P1)}$, $Slice_1^{(P2)}$, ……….$Slice_1^{(PM)}$
t_2	$Slice_2^{(P1)}$, $Slice_2^{(P2)}$, ……….$Slice_2^{(PM)}$
. . t_N	$Slice_N^{(P1)}$, $Slice_N^{(P2)}$, ……….$Slice_N^{(PM)}$

The concurrent operation timing diagram in shown in figure 5.

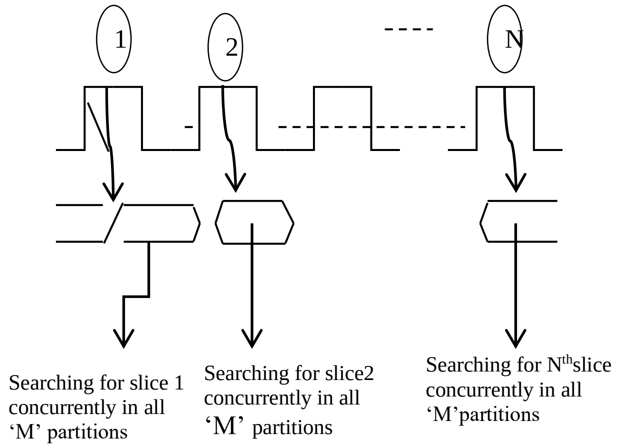


Figure 5 Timing diagram for slice searching

Visual crypto being the process of peeling the partitions in original image and grouping the portions, structure theorem can be stated as follows.

A. Structure Theorem:

The individual elements in a group are commutative and abelian. The complete image is the addition of the individual expressed as $G \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3} \dots\dots \mathbb{Z}_{n_k}$

If there are five elements in each sub group,then it corresponds to $\mathbb{Z}_5$ = {0,1,2,3,4} the natural numbers upto (n_5-1) and totally there are five elements in $\mathbb{Z}_5$. Similarly, $\mathbb{Z}_2 \rightarrow$ consists of 0's and 1's and $\mathbb{Z}_4 \rightarrow$ consists of 0,1, 2 and 3.

Thus, size of elements in G is the product i.e. n_1, n_2 ……n_K.

The original image and the visual crypto subgroups also satisfy the isomorphism property:

Isomorphism (Equality of groups)

$G \simeq H$ If ∃a bijection:: G→H one-one correspondence between G & H and ≃ is the isomorphic operator. The satisfied properties include

$\varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2)$

where the multiplication in left (right) side is in G (H).

B. Transformation method:

Totally 'N' frames exist and morphism from one group to another is done. For ex:$\mathbb{Z}_4 is = \mathbb{Z}_2 \oplus \mathbb{Z}_2$

1st frame classified as $\mathbb{Z}_2$ as (0, 0) (0, 1) (1, 0) and (1, 1) i.e. 4 sub frames

In $\mathbb{Z}_4$ 1+1+1+1 =0 mod(4)and also 3+3+3+3 = 0 mod (4)

In $\mathbb{Z}_4$d(1) =d(3) = 4 i.e. the minimum number of times '1' should be added to get 0 after mod(4).

Similarly, d(2)=2 i.e. 2+2 = 4 and mod(4)=0. The identity elements is obtained by adding two terms of element 'z' to get the identify element in $\mathbb{Z}_4$ i.e. '0'. Three transformations applied to visual crypto with original image in 12 partitions are.

Case (i) Subgroups in $\mathbb{Z}_4$ and cosets in $\mathbb{Z}_3$

$P_1 = \{0, 3, 6, 9\} \simeq \mathbb{Z}_4$

And Cosets are $\{P_1, 1 + P_1, 2 + P_1\} \simeq \ni \mathbb{Z}_{12}/P_1 \simeq \mathbb{Z}_3$

The crypto frames are $\{0, 3, 6, 9, 1, 4, 7, 10, 2, 5, 8, 11\} \simeq \mathbb{Z}_{12}$

Case (ii) Subgroups in $\mathbb{Z}_3$ and cosets in $\mathbb{Z}_4$

L = {0, 4, 8} $=\mathbb{Z}_3$

The Cosets are $\{L, 1 + L, 2 + L, 3 + L\} \simeq \ni \mathbb{Z}_{12}/L \simeq \mathbb{Z}_4$

The crypto frames are {0, 4, 8, 1, 5, 9, 2, 6, 10, 3, 7, 11}

Case (iii) Subgroups in $\mathbb{Z}_6$ and cosets in $\mathbb{Z}_2$

$M = \{0,2,4,6,8,10\} \simeq \mathbb{Z}_6$

Cosets are $\{M, 1 + M\} \ni \mathbb{Z}_{12}/M \simeq \mathbb{Z}_2$

The crypto frames are {0, 2, 4, 6, 8, 10, 1, 3, 5, 7, 9, 11}

Figure 6 shows the destegano method.

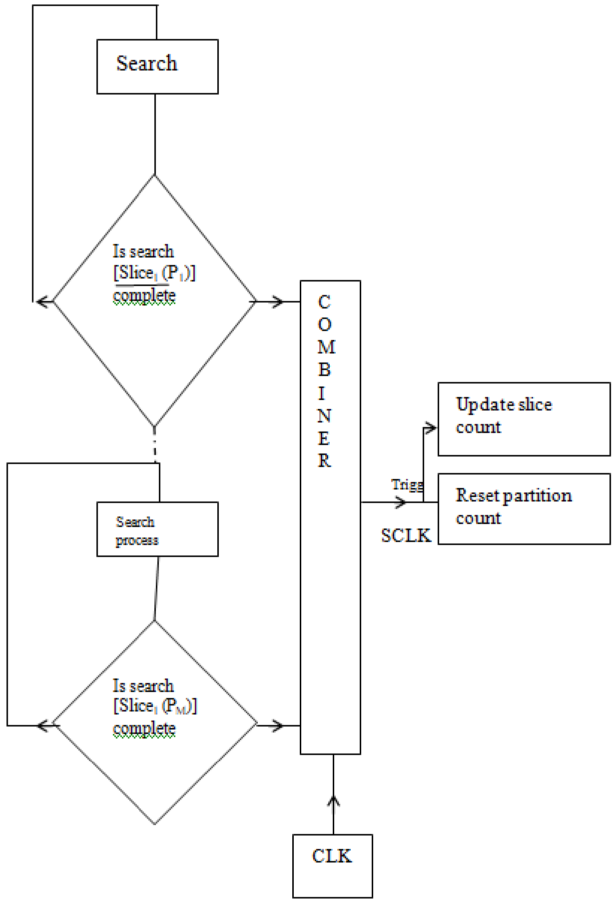


Figure 6 The destegano process

IV. EXPERIMENTAL RESULTS

The execution time of the proposed algorithm is compared with standard algorithms like DES and AES and the results are tabulated in Table 4.

Table 4 Execution time comparison for Encryption

original file size(kb)	Execution time of proposed algo(ms)	Execution time for DES(ms)	Execution time for AES(ms)
18	925	1098	1205
20	968	1148	1268
22	1134	1189	1298
24	1168	1287	1306

It can be seen that the proposed algorithm reduces the execution time(ms) compared to standard algorithm like AES and DES.

Table 5 Encrypted file size comparison

original file size(kb)	Image share size of proposed algo.(kb)	Encrypted file size for DES(kb)	Encrypted file size for AES(kb)
18	3	18	18
20	3	20	20
22	6	22	22
24	6	24	24

Table 5 shows the encrypted file size for the proposed algorithm which is compared with AES and DES. It can be seen that the encrypted file size has reduced as only size of image share are considered. The verilog implementation results are shown in figure 7. Encryption process execution time comparison

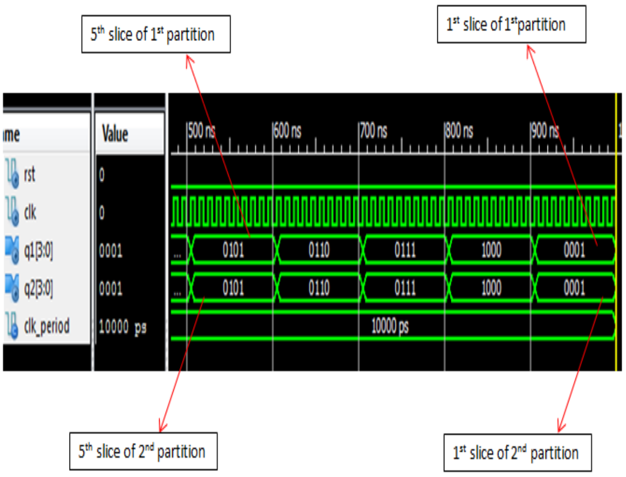


Figure 7 Verilog Implementation

VI. CONCLUSIONS

An algorithm for PPDM using visual cryptography was proposed and implemented in this work. The step by step procedure of the proposed algorithm is discussed and implemented. Verilog implementation of the algorithms has been done. Proposed future work is to implement these algorithms in mobile phones,.

REFERENCES

1. Ching-Nung Yang, Li-Zhe Sun, Song-Ruei Cai (2016) "Extended color visual cryptography for black and white secret image", Theor. Comput. Sci.609:143-161.
2. Ching-Nung Yang, Che-Yu Lin (2015) "Almost-aspect-ratio-invariant visual cryptography without adding extra subpixels", Information Sciences.312: 131-151.
3. Xuehu Yan, Shen Wang, Xiamu Niu, Ching-Nung Yang (2015) "Generalized random grids-based threshold visual cryptography with meaningful shares". Signal Processing,109:317-333.
4. Pei-Yu Lin, Ran-Zan Wang, Yu-Jie Chang, Wen-Pinn Fang(2015), "Prevention of cheating in visual cryptography by using coherent patterns", Information Sciences, 301: 61-74.https://doi.org/10.1016/j.ins.2014.12.046
5. Pei-Ling Chiu,Kai-Hui Lee (2015), "User-friendly threshold visual cryptography with complementary cover images". Signal Processing.108: 476-488.
6. Xuehu Yan, Shen Wang, Xiamu Niu, Ching-Nung Yang(2015) "Half tone visual cryptography with minimum auxiliary black pixels and uniform image quality" .Digital Signal Processing, 38:53-65.
7. Duanhao Ou, Wei Sun, Xiaotian Wu (2015),"Non-expansible XOR-based visual cryptography scheme with meaningful shares", Signal Processing,108: 604-621.
8. Roberto De Prisco, De Santis, A (2014), "On the Relation of Random Grid and Deterministic Visual Cryptography". IEEE Transactions n Information Forensics and Security.9(4): 653 – 665.DOI: 10.1109/TIFS.2014.2305574
9. Khandelwal N.S, Kamboj P (2015) "Two factor authentication using Visual Cryptography and Digital Envelope in Kerberos". International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Print ISBN: 978-1-4799-7676-8, DOI: 10.1109/EESCO.2015.7253638

AUTHORS PROFILE

P.Subhashree has done M.E at Anna University of Technology, Trichy and B.Tech at JJCET Trichy. She had 6+ years of teaching experience. Currently she is pursuing Ph.D. at Sathyabama Institute of Science and Technology. Chennai.

Dr.G.Gunasekaran, Principal J.N.N Institute of Engineering Chennai, has obtained his B.E from National Engineering College and M.E from Jadavpur University and Ph.D. also from the same University and he has published 13 International Journals and has attended 7 International Conferences. He has got a profound experience of 27 years.