International Journal on Emerging Technologies 11(3): 634-638(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Key Generation using Featured based Finite Element Method

Chandra Prakash Singar[1], Jyoti Bharti[2] and R.K. Pateriya[3]
[1]Assistant Professor, Department of Information Technology,
Shri G.S. Institute of Technology & Science Indore (Madhya Pradesh), India.
[2]Assistant Professor,Department of Computer Science and Engineering,
Maulana Azad National Institute of Technology Bhopal (Madhya Pradesh), India.
[3]Associate Professor, Department of Computer Science and Engineering,
Maulana Azad National Institute of Technology Bhopal (Madhya Pradesh), India.

(Corresponding author: Chandra Prakash Singar)
(Received 04 March 2020, Revised 20 April 2020, Accepted 25 April 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The Finite Element Method (FEM) has turned into an effective and well known apparatus to tackle the problems and find the solution of Engineering, Mathematics and in various traits numerically. Generally this FEM also know as finite element analysis (FEA). Due to mathematical nature, now it is used to extract the features of an image. In this paper we highlighted the method of key generation that is based on feature extraction and the feature are extracted using novel method called finite element method. The feature of matrices using FEM is a displacement vector. The displacement vector features are computed using element stiffness matrix, global stiffness matrix and equilibrium equation. The obtained result on image matrices and shuffling the values of a matrix either column wise and rows wise then the Feature Displacement Vector (FDV) almost are same. To extract the feature in an image a novel method has been introduced called featured based finite element method (FFEM). We analyzed all the features of FEM and generate unique key that is used in application of cryptography.

Keywords: FEM, FEA, FEB, FFEM, ESM, GSM.

Abbreviations: FEM, finite element method; FEA, finite element analysis; FEB, finite element blocks; FFEM, featured based finite element method; ESM, element stiffness matrix; GSM, global stiffness matrix;

I. INTRODUCTION

The communications play a vital role in information processing. The rapid uses of the network make this communication much easy or sophisticated. The secure network made much easier and reliable communication and therefore the forwarding of information from one sender to another one to be more protected [2]. The method used for secure communication is cryptography. Besides the method implemented for data encryption and decryption is well-known to everyone, however the confidential exchangeable key generation would be problematic to predict, and it should be unknown from the third party (intruder). For secure transfer of information, generation of secret key has many challenges more ever this problem can be solved if the both communicating party exchange the secret key in another form or if encryption and decryption process used separate secret key for each process, however the approach of generating the secret key from an image came to the role. For finding the approximate solution of a given problem in the mechanics area of deformable solids Ritz developed an effective method. The method used different estimate calculation of energy functional unknown coefficients with the help of identified function [1]. Even though this method has been widely used earlier in domain of structural mechanics, now at that time this method also applied for the solution of more than a few other kinds of engineering problems like electrical and magnetic fields, boundary detection and a lot of additional area. FEM also used in practical applications of engineering such that this FEM also called Finite Element Analysis (FEA). An application of this FEA used to analysis the different computations of engineering and moreover this also used as a computational tool for analysis. Mesh generation techniques can be used for subdividing a difficult problem domain into small elements. Finite element analysis is better solution for analyzing problems over complex domains, whenever the present domain changes from solid shape to a moving edge; the precision of this domain varies over the complete domain. The finite element method (FEM) can be used as a numerical method for providing solution of different problem in the field of engineering and various other areas [3]. Moreover these methods also know as finite element analysis (FEA). Due to the partial differential equation, the analytical and boundary value problems are resolved. To solve the given problem, at the first steps it divides a big problem into smaller ones. The undersized portion called finite elements. However the mathematical equations of particular finite elements are then grouped together to a larger structure which forms the model of the given problem [3]. FEM uses variations in given problem and finding approximation solution by normalizes an error. The FEM differential equations are also used in medical imaging and computer vision domain.

Feature Extraction: Feature plays an awfully necessary role among the domain of image processing. In this technique basically transforming the input stream that output can be used as a set of feature is called

feature extraction. These techniques can be applied to recommend that is helpful in classifying and recognition of image data. It is the more relevant technique for dimensionality reduction [4]. The objective of feature extraction is to obtain more related raw information from the real data and more ever that data can be represent information in to a minor dimensionality space. The process of feature extraction get extracts more relevant features from objects to form as a feature vectors. However this feature vectors are then used in the process of classification and pattern recognition of image data.

Classification of FEM with other methods: The available methods for the solution of general field problems, like elasticity, fluid flow, heat transfer problems etc. The classification of different method as presented in Fig. 1 [1]. The method for finding approximate solution can be dividing into two separate field analytical analysis and numerical analysis, this method further classified in to different sub domain.

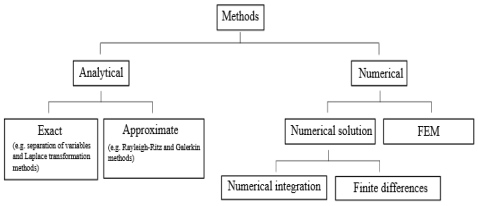

Fig. 1. Classification of common methods [1].

Finite element methods and its types:

— Applied Element Method: In this method it combines all the features getting from both method FEM and DEM know as discrete element method. Moreover the applied element method used as a numerical analysis for prediction the rang and the discrete behaviors of the structure.

— Generalized Finite Element Method: This method uses as local spaces consist of functions, which reflect at present available information from unknown solution and thus ensure to getting enhanced local approximation.

— Mixed Finite Element Method: In this method extra independent variables are used as new nodal variables during the process of discretization for partial differential equation problem.

— Hp-FEM: It is a very basic method of FEM. The main functions of this method are adaptively. The value of variable size h and polynomial degree (p) getting the result more accurate and fast, and probably up to exponential convergence rates.

— Extended Finite Element Method: This method also combination of two method. Basically the XFEM method is based on numerical procedure that uses two most common methods that is GFEM (generalized finite element method) and the partition of unity method. It is extension of the new classical finite element method by enriching the solution space for solutions to differential equations with discontinuous functions.

— Smoothed Finite Element Method: The S-FEM is a numerical simulation method which used to simulate of physical phenomena.

II. LITERATURE SURVEY

Seshadri and Trivedi (2011) suggested efficient ways of key generation method using biometric templates. Moreover, the traditional encryption keys are large in nature and it is very hard to keep in mind [5]. Further the proposed work for the generation of cryptographic key, author used finger prints templates. In this method three different processes are used first key release, second key binding and finally get the key generation. Wu *et al.,* (2010) proposed a secure in nature and stable binary key generation algorithm using images. Face biometrics images are used to extracts the different facial feature because biometric feature uniquely classifies the different facial features [6]. At the time of encryption process the feature of facial features are extracted, and generated key is further encrypted. Omerasevic *et al.,* (2013) the fundamental though of this work is original message shared between two parties with the help of generate cryptography key [7]. However the size of specified key and space is unbounded. In this process original information is encoded independently with the distinctive key, the generated key will be same as one time padding. In addition, this method generates various keys i.e. cryptographic keys with variable size in nature. Yang *et al*., (2011) suggested method extracting the different features value from SAR images that is based on the co-occurrence matrix [8]. Freire-Santos (2006) suggested in the proposed work that is based cryptography key generation algorithm by handwritten signature [9]. The fuzzy vault is being used to implement in the signature based key generation technique. Beng *et al.,* (2008) design key generation system that is based on biometric images. The fundamental idea of the proposed work based on basis of a randomized biometric helper. Moreover the randomized nature of this helper guarantees that generated keys are extremely simple to be rescinded when third party compromise the secret key [10]. Nandini and Shylaja (2011) implemented the proposed approach is based on unique method for secure key generation. The authors suggested key generation using hashing method that is symmetric hash function for different users further this method is better in terms of security and speed [11]. Ogiela and Ogiela (2011) the fundamental idea of the proposed work focus on generation a key based on visual pattern that contain personal data. Generated key can be recognized by different user features, and this features used by individual person. In this work, the generations of key using palm image of user are presented [12]. Giovannelli *et al*., (2013) suggested in this method that finite element method being used as a numerical method for providing fairly accurate solutions for particular problem, problems behavior can be described with the help of differential equations, such as the calculation of the displacement and stress fields in a structural component under known boundary conditions [13]. In this paper, detect the boundary of an object by using nested Cartesian grid. Karaolani *et al.,* (1989) FEM uses the energy integral directly, and works by dividing the given domain into sub domains and minimizing the energy integral over each sub domain separately [14]. This produces the so called "element equations" which are then joined together through their common boundaries. External forces which are free of the unknowns to be resolved may be represented in FEM as an arrangement of loading conditions. A simple artery model can be specified by minimizing the energy integral given in expression. Wang *et al*., (2011) suggested that the updating of finite element model includes the examination of hypothetical expectations

with test estimations. In auxiliary elements, the information usually takes the variety of different natural frequencies, mode shapes and damping coefficients. In the calculation of finite element the Eigen vectors are usually calculated by compare it with a calculated mode shape at certain grid [15]. The correlation mode shapes measurement is along with these lines and the quantity of measured point and their choice is an important issue considered in various studies, regularly. Preuber and Rumpf (2000) finite element methods are suitably executes the diffusion based models [16]. The connected finite elements in a variation way to deal with image processing. In the various areas of scientific computing, the techniques associated with finite element have been joined to liberally lessen the necessary degree of flexibility while sparing the gauge idea of the numerical solution. In this manner the estimators that are defined locally or the error markers that steer the refined grid locally and separately were coarsening. Li *et al.*, (2018) in this work the author proposed a method with deep leaning concept. Using deep leaning technique it classifies and extract the feature from iris templates. The suggested technique show improved result among different method and compare with existing work [17]. Prabuwono *et al.*, (2019) the key idea of this suggested work uses combination of methods to generate different feature extraction from image and it identifies the facial feature. Content based image retrieval focus on image by the exploiting the various features. This method uses different coordinate value from texture and color for generating feature extraction [18]. Sharma and Shrivastava (2019) author proposed a deep learning approach for features extraction; deep features are extracted from the pre-trained convolutional neural network using shape and texture. In this proposed method author also uses the histogram of oriented gradient and Gabor [19]. Anandh and Indirani in this work, features are extracted from image using directional local ternary quantized extrema pattern. Then, the extracted features is classify with the help of multi-class support vector machine [20].

III. PROPOSED MEHODOLOGY ANDALGORITHM

*– Choose gray scale image I_1 of size (m*n).*
*– Divide the image I_1 into size of (2*2), called finite element blocks (FEB).*
– Now, find the node of each block, value of each node is the average of all pixels of each block.
– Calculate the element stiffness matrix (K_n),

$$K_n = \frac{E.A}{L}\begin{bmatrix} P & Q \\ R & S \end{bmatrix}$$

– Now, combining the entire element stiffness matrix, called global stiffness matrix (K_e).
– Solve the equilibrium equation,

$$[Ke] * \vec{Q} = \vec{F}$$

– After solving the equilibrium equation, get the values of displacement vector ($Q_1, Q_2 \ldots Q_n$).
– Get more value of displacement vector, after shuffling of rows and columns.

First we choose the matrix of size (4*4). Fig. 3 (a) and (b) shows the original matrix and nodes of a matrix respectively. Now divide the image into blocks of size (2*2) called finite element. After dividing the image matrix, create nodes of each block. Now evaluate the Element Stiffness Matrix (Kn). Young modulus E =0.65 and Force vector [-77.65, 14.60, 14.60, 388.46, 65.59].

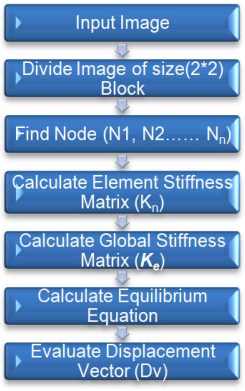

Fig. 2. Proposed Methodology.

For Example:

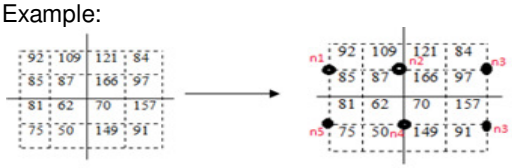

Fig. 3(a) Matrix (4*4) **(b)** Create Nodes.

Here Node value is calculated by averaging the pixel value of each finite element shown in Eqn. 1.

Average (Ni) $= \frac{1}{n}\sum_{i=0}^{n} P_i$. (1)

Here N1=93.25,N2=101,N3=116.75,N4=67,N5=93.25 and the value of next node N3 is equal to the value of previous node N3.similarly $N_5 = N_1$.Now calculate the cross sectional area (A1, A2, A3, A4) of each finite element. The value of A_1=97.125 (Averaging of N_1andN_2). Similarly, A_2 = 108.5, A_3 = 91.875 andA_4 = 80.125 and the length of every block (L_i) is equal to 2. Now evaluate the Element Stiffness Matrix (K_n) of each Finite Element.

$$K_1 = \frac{E_1 A_1}{L_1}\begin{bmatrix} 92 & 109 \\ 85 & 87 \end{bmatrix} = \frac{0.65*97.125}{2}\begin{bmatrix} 92 & 109 \\ 85 & 87 \end{bmatrix}$$

$$= 31.56\begin{bmatrix} 92 & 109 \\ 85 & 87 \end{bmatrix} = \begin{bmatrix} 2903.52 & 3440.04 \\ 2682.6 & 2745.72 \end{bmatrix}$$

Similarly

$$K_2 = \begin{bmatrix} 6564.25 & 4557 \\ 9005.5 & 5262.25 \end{bmatrix}, K_3 = \begin{bmatrix} 66.5 & 149.15 \\ 141.55 & 86.45 \end{bmatrix}$$

and $K_4 = \begin{bmatrix} 39.69 & 30.38 \\ 36.75 & 24.5 \end{bmatrix}$

Now calculate the Global Stiffness Matrix [K_e].

$[K_e] = K_1+K_2+K_3 \ldots\ldots\ldots\ldots\ldots\ldots K_n$. After assembling all the Element Stiffness Matrix, we get,

$$\begin{bmatrix} 2903.52 & 3440.04 & 0 & 0 & 0 \\ 2682.6 & 8007.97 & 4557 & 0 & 0 \\ 0 & 9005.5 & 5328.75 & 149.15 & 0 \\ 0 & 0 & 141.55 & 126.14 & 30.38 \\ 0 & 0 & 0 & 36.75 & 24.5 \end{bmatrix}\begin{bmatrix} Q_1 \\ Q_2 \\ Q_3 \\ Q_4 \\ Q_5 \end{bmatrix} = \begin{bmatrix} -77.65 \\ 14.60 \\ 14.60 \\ 388.46 \\ 65.59 \end{bmatrix}$$

On solving, the equilibrium equation, we get Q_1 = 1.45, Q_2 = 0.89, Q_3 = 0.53, Q_4 = -0.92, Q_5 = 1.53. After shuffling of rows and columns, get more values of displacement vector.

IV. RESULT ANALYSIS

The proposed methodology, FFEM is simulated on matlab 2015 (a). To extract the features of image matrices, the feature of matrices using FEM is a displacement vector. From the obtained result on image matrices and shuffling the values of a matrix either column wise and rows wise shown in Table 1 and 2. When we shuffle the value of column wise C1 to C2 and C3 to C4, then the feature displacement vector (FDV) almost are same with negligible difference except Q2, but the values are not same. All the features value on shuffling and get the different values. As per Table 2, the result of row wise shuffling is similar pattern has been found of column wise and all the feature values of row wise and column wise are unique. As per Fig. 4 and 5, feature displacement vector values are lies between 0 - 2.

Table 1: Column wise shuffling.

Column	original	$C_1 \leftrightarrow C_2$	$C_1 \leftrightarrow C_3$	$C_1 \leftrightarrow C_4$	$C_2 \leftrightarrow C_3$	$C_2 \leftrightarrow C_4$	$C_3 \leftrightarrow C_4$
Q1	1.45	1.46	1.87	1.47	1.85	1.40	1.45
Q2	0.89	0.89	0.70	0.89	0.74	0.94	0.94
Q3	0.53	0.52	0.61	0.77	0.76	0.76	0.53
Q4	- 0.92	0.92	0.76	0.72	0.65	0.61	0.91
Q5	1.53	1.53	1.50	1.55	1.54	1.50	1.55

Table 2: Row wise shuffling.

Rows	original	$R_1 \leftrightarrow R_2$	$R_1 \leftrightarrow R_3$	$R_1 \leftrightarrow R_4$	$R_2 \leftrightarrow R_3$	$R_2 \leftrightarrow R_4$	$R_3 \leftrightarrow R_4$
Q1	1.45	1.46	1.22	1.14	1.34	1.28	1.45
Q2	0.89	0.94	0.96	0.96	0.85	0.86	0.89
Q3	0.53	0.53	0.64	0.67	0.59	0.61	0.52
Q4	- 0.92	0.92	0.86	0.84	1	0.96	0.91
Q5	1.53	1.56	1.53	1.53	1.55	1.53	1.52

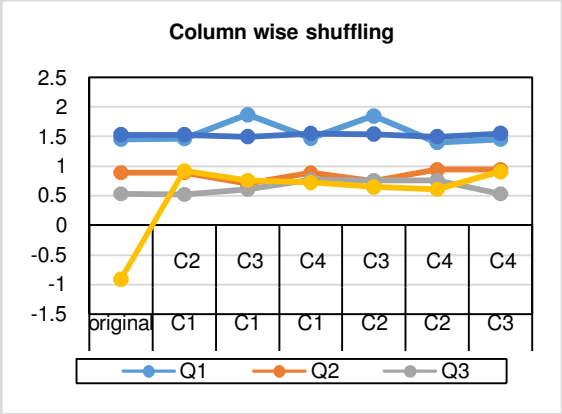

Fig. 4. Graph for Displacement Vector of column shuffling.

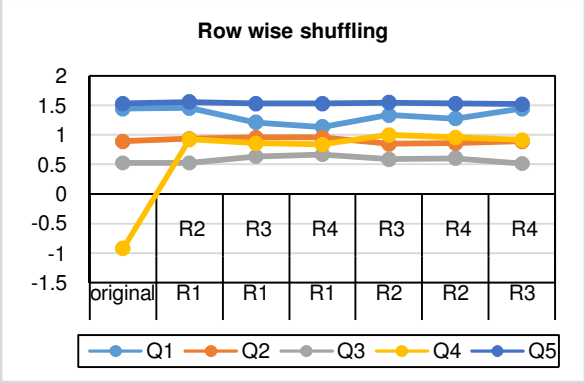

Fig. 5. Graph for Displacement Vector of row shuffling.

V. CONCLUSION

In this paper we propose a novel technique for key generation using featured based finite element method for image. The security of image depends on the security of the key. Mostly the feature displacement vector is unique and does not produce the similar kind of pattern of values. So this displace vector is used to extract the features of an image matrix. Furthermore the key is generated according to the different equation that is displacement vector features computed using element stiffness matrix, global stiffness matrix and equilibrium equation. To extract the feature of the image we calculate different displacement vectors.

VI. FUTURE SCOPE

Future research scope in the field belongs to the machine learning application where featured are extracted using complex mathematical equations.

REFERENCES

[1]. Barkanov Evgeny (2001). Introduction to the finite element method. Institute of Materials and Structures Faculty of Civil Engineering Riga Technical University.

[2]. Priyanka, M., Kumari, R. L., Lizyflorance, C., & Singh, K. J. (2013). A New Randomized Cryptographic Key Generation Using Image. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, *2*(6), 2319-5967.

[3]. Jacob, F., & Ted, B. (2007). *A first course in finite elements*. John Wiley & Sons, Ltd.

[4]. Kumar, G., & Bhatia, P. K. (2014, February). A detailed review of feature extraction in image processing systems. In *2014 Fourth international conference on advanced computing & communication technologies*, 5-12.

[5]. Seshadri, R., & Trivedi, T. R. (2011). Efficient cryptographic key generation using biometrics. *International Journal of Computer Technology and Applications*, *2*(1), 183-187.

[6]. Wu, L., Liu, X., Yuan, S., & Xiao, P. (2010). A novel key generation cryptosystem based on face features. In *IEEE 10th International Conference on Signal Processing Proceedings*, 1675-1678.

[7]. Omerasevic, D., Behlilovic, N., & Mrdovic, S. (2013). CryptoStego-A novel approach for creating cryptographic keys and messages. In *2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP),* 83-86.

[8]. Yang, K. Z., Cheng, Y. L., & Liu, J. (2011). A Method for Extracting the Text Feature of SAR Image Based on Cooccurence Matrix. In *2011 4th International Congress on Image and Signal Processing, 4*, 2038-2043.

[9]. Freire-Santos, M., Fierrez-Aguilar, J., & Ortega-Garcia, J. (2006). Cryptographic key generation using handwritten signature. In *Biometric technology for human identification III* (62020N), 225–231. International Society for Optics and Photonics.

[10]. Beng, A., Teoh, J., & Toh, K. A. (2008). Secure biometric-key generation with biometric helper. In *2008 3rd IEEE Conference on Industrial Electronics and Applications*, 2145-2150.

[11]. Nandini, C., & Shylaja, B. (2011). Efficient cryptographic key generation from fingerprint using symmetric hash functions. *International Journal of Research and Reviews in Computer Science*, *2*(4), 937-942.

[12]. Ogiela, M. R., & Ogiela, L. (2011). Image based crypto-biometric key generation. In *2011 Third International Conference on Intelligent Networking and Collaborative Systems*, 673-678.

[13]. Giovannelli, L., Marco, O., Navarro, J., Giner, E., & Ródenas, J. (2013). Direct creation of finite element models from medical images using Cartesian grids. *Computational Vision and Medical Image Processing IV: VIPIMAGE 2013*, 167.

[14]. Karaolani, P., Sullivan, G. D., Baker, K. D., & Baines, M. J. (1989). A Finite Element Method for Deformable Models. In *Alvey Vision Conference*, 1-6.

[15]. Wang, W., Mottershead, J. E., Ihle, A., Siebert, T., & Schubach, H. R. (2011). Finite element model updating from full-field vibration measurement using digital image correlation. *Journal of Sound and Vibration*, *330*(8), 1599-1620.

[16]. Preuber, T., & Rumpf, M. (2000). An adaptive finite element method for large scale image processing. *Journal of Visual Communication and Image Representation*, *11*(2), 183-195.

[17]. Li, X., Jiang, Y., Chen, M., & Li, F. (2018). Research on iris image encryption based on deep learning. *EURASIP Journal on Image and Video Processing*, 1-10.

[18]. Prabuwono, A. S., Usino, W., Bramantoro, A., Allehaibi, K. H. S., Hasniaty, A., & Defisa, T. (2019). Content Based Image Retrieval and Support Vector Machine Methods for Face Recognition. *TEM Journal*, *8*(2), 389-395.

[19]. Sharma, A. K., & Shrivastava, A. (2019). Cross Spectral Face Recognition using Handcrafted and Deep Features. *International Journal of Electrical, Electronics. and Computer Engineering, 8*(1), 18-24.

[20]. Anandh, R., & Indirani, G. (2020). IoT and Cloud based Feature Extraction and Classification Model for Automatic Glaucoma Detection. *International Journal on Emerging Technologies, 11*(2), 13-18.

How to cite this article: Singar, C. P., Bharti, J. and Pateriya, R. K. (2020). Key Generation using Featured based Finite Element Method. *International Journal on Emerging Technologies*, *11*(3): 634–638.