International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Autonomous Data hiding in an Encrypted Image using KM-DH Algorithm

S.Janani, M.Shalini, K.Parkavi, A.Chandrasekar

Abstract: ***K Means Clustering (KM) based data hiding algorithm (KM-DH) is to perform cluster operation which means split pixels into chunks from already encrypted image. Under Consideration of splitted pixels find place to allocate information Authenticated person encrypt the image pixels with their key to prepare envelope image then flow goes by grouping the pixels to stuff the already encrypted image of lowest bits to generate place to allocate data using K means Clustering methods with the help of secret key it form split up matrix.In Receiver side after getting the encrypted data they can withdraw data and image separately without overlapping each other using data and image encryption key.At the same time receiver can also get both the image and data without any bug by dimensional link.***

Keywords: KM-DH algorithm,Encryption,Secret key

I. INTRODUCTION

Nowadays, the data transmission across the internet are growing fastly day by day. The valuable data such as personal image, confidential audio and video, authenticated data's etc are must be protected from vulnerable activity. Because data theft are increasing tremendously in this channel. We are all facing so many forgery, data loss and data theft due to insecure communication link and also many security problems are available in many websites. In this the main problem we have to focus in the area of data confidentiality and data authentication. There are various mechanisms are available for data hiding such as symmetric key encryption, Asymmetric key Encryption, Hashing techniques and digital signature.

II. RELATED WORKS

Using secret key stenographic messages are encoded and then a cover image is altered into encoded message. The recognition of steganographically encoded bundles is called steganalysis.[1], Three algorithms are available. It is difficult to remove the necessity of specifying the k value in further but the first algorithm perform those functioning its bring about ideal number of cluster.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
S.Janani*, Computer Science and Engineering, St.Joseph's College Of Engineering, Chennai, India. Email:sjanani.me@gmail.com
M.Shalini, Computer Science and Engineering, St.Joseph's College Of Engineering, Chennai, India. Email:shalini.mathi@gmail.com
K.Parkavi, Computer Science and Engineering, St.Joseph's College Of Engineering, Chennai, India. Email:Nancy.parkavi@gmail.com
A.Chandrasekar, Computer Science and Engineering, St.Joseph's College Of Engineering, Chennai, India. Email:drchandrucse@gmail.com

Second design decrease computational unpredictability and delete dead unit issue. It choose the most populated zone as cluster region. Plain data structure is used to stock data in every of the looping and then in the successive looping by third algorithm.[5],Using image preprocessing technique, it detect and remove noises present in the image. Converting original input image into three different stages (RED,BLUE,GREEN).Embedding takes place after stage separation at the same time secret key is embedded with data extraction and embedding process. Its difficult to decode the data without knowing the keys[7],Encrypted image pixels are stretched with the help of spilt-up matrix A_{ij} to allocate the memory place for data hiding using the proposed K means clustering algorithm in these case data can be hidden in the picture and the end user can get information and picture autonomously with their relating keys.

III. PROSPOSED SYSTEM

In proposed system there are three modules available. Two module comes under sender side and third module comes under receiver side. They are picture encryption, data encryption and data decryption and picture extraction. On Sender side, the authenticated person encrypt the original picture with the help of the encryption key. After getting the encrypting picture it undergone into KM mechanism to perform clustering process to get pixels and split up matrix. In this duration it produces LSB of the encrypted image using data encryption password to generate the place for information covering up. On recipient side, they can easily decrypt and get the data using decryption key in generated place from the encrypted picture. The changes in the Lowest bit doesn't affect the original picture quality. In other hands, its also possible to decrypt both the content and image as well.

A. Encrypt Picture using secret key

In an picture the bit plane refers binary values for all pixels. Take the original picture, find out the lowest bits in the picture in each pixels. In Lowest bits insertion have either 24 bit color or 8 bit color. Every pixel can have one in 2^24 colors or 2^8 colors given by 8 bits each. Gray scale value carries intensity information such that, consider

Show the gray value as $AB_{i,j}$, where i,j indicates the pixel position, and pixel bits denoted as $c_{i,j,0}$, $c_{i,j,1}$, …, $c_{i,j,23}$ or $c_{i,j,0}$, $c_{i,j,1}$, …, $c_{i,j,7}$ The gray value is converted into bits by converting

$AB_{ij}=(ACi,j,k/2^{k)}$ Mod 2. K=0,1,2…..27

Perform encryption using XOR operation $AC_{i,j,k}$ with each pixel of an picture

$$AB_{i,j,k} = BC_{i,j,k} \sim AC_{i,j,k}$$

B. Data Insertion with Encrypted image

Here insert data in a randomly interchanged position of the pixels and tamp it with the spilt up matrix to allocate a place for locating data by using KM Mechanism

---

Algorithm: Data hiding in KM Mechanism

READ *CI Original (encrypted) picture,* $D_{[1,\ldots n]}$ *Text, and K Secret key*
RESULT *picture Text.*
SET *variables O,P and I*
Choose V_p*/V pixels from CI Variables*

$AB_{ij}=A_{ij\%}Bij$
$P= [V\text{-}V_p]^{p(k)}$
$G= [V\text{-}Vp]/P$
$I=0$
While
for *j in range of(o,p)*
for *k in range of(o,m)*
$Lowerbit_{i,j}= A_{j,k}$
endfor
endfor

$cbits_{i,1..M.L\text{-}I}$ $=Lowerbit\ i,1,\ldots,\ Lowerbit\ i,M.PL\text{-}I$
$PM_{i,1\ldots I}$ $=$ $Lowerbit\ i,O.PL\text{-}I*1,\ldots\ldots,\ Lowerbit\ i,O.PL$
$PM_{i\ldots G,1\ldots I}$ $= [unicode(D_{[1,\ldots nj]})]/2^k \bmod 2\ ,\ k=1,..,7$
$p = [V\%V_p]$
return *CI containing* $D_{[1,\ldots\ldots,n]}$

C. Both data and Picture retrieval

In receiver end, the receiver can have the option to retrieve data or picture or both. Due to the randomly chosen pixels we can choose selection and transformation is easier and at the same way intruder can't find the data without knowing the secret key. Because the region values and pixels group are varying randomly so it is difficult to retrieve the data. In addition to that, the reverse process is really convenient for the authorized user to retrieve the data as well as picture. Therefore the reverse process of KM mechanism for data hiding is easier. At the same time receiver can also get both the image and data without any bug by dimensional link.

IV. EXPERIMENTAL RESULTS

Given below figure1(a) is the original image whereas after encrypting the picture with 24 bit of each pixel are reversed into a gray scale value to prepare an encoded picture figure1(b).The encrypted picture is used for hiding the data using KM mechanism As shown in figure.1(c).After encrypting the data and the picture the receiver can retrieve the data separately without affecting the image quality and the same time it is also possible to retrieve image without decrypting the data.

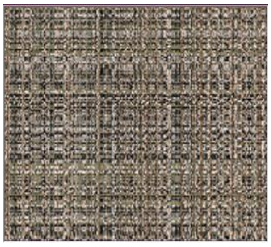

Fig. 1(b) **Fig. 1(a)**

Figure. 1(a) Koala.jpg Figure. 1(b) Encrypted picture

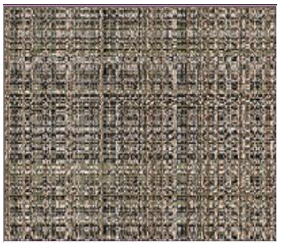

Figure. 1(c) Figure. 1(d)

Fig. 1(c) picture hiding data Fig. 1(d) Decrypted image

By using both the data-hiding and the encoded keys, the embedded data could be decoded efficiently and the original image could be perfectly recovered from the encrypted image containing embedded data.

V. CONCLUSION

K means clustering data hiding mechanism is used for data hiding and picture encryption without affecting the original quality of the picture. With the help of the spilt-up matrix the encrypted pictures pixel scale used to allocate the place for data hiding. The receiver can extract the data or they can retrieve picture or both data and picture without any correlation and bugs

REFERENCES

1. Chandreyee Maiti* , Debanjana Baksi, Ipsita Zamider, Pinky Gorai, and Dakshina Ranjan Kisku," Data Hiding in Images Using Some Efficient Steganography Techniques" T.-h. Kim et al. (Eds.): SIP 2011, CCIS 260, pp. 195–203, 2011. © Springer-Verlag Berlin Heidelberg 2011
2. Afrakhteh, M., & Ibrahim, S. "Adaptive steganography scheme using more surrounding pixels". Paper presented at the Computer Design and Applications (ICCDA), 2010 International Conference on (2010, 25-27 June 2010).
3. Ramadhan Mstafa, Christian Bach," Information Hiding in Images Using Steganography Techniques"ASEE Northeast Section Conference Norwich University Reviewed Paper March 14-16, 2013
4. Huda Hamdan Ali , Lubna Emad Kadhum," K- Means Clustering Algorithm Applications in Data Mining and Pattern Recognition", ernational Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 6 Issue 8, August 2017.
5. Jyoti Yadav , Monika Sharma," A Review of K-mean Algorithm", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 7- July 2013.
6. Abikoye Oluwakemi ,Adewole Kayode S., Oladipupo Ayotunde J."Efficient Data Hiding System using Cryptography and Steganography "International Journal O Applied Information Systems,ISSN:2249-0868,Volume 4-No.11,December 2012.
7. Xinpeng Zhang,"Reversible Data Hiding in Encrypted Image", EEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011.

8. Anandaprova Majumdera, Suvamoy Changderb ,"A Novel Approach for Text Steganography: Generating Text Summary using Reflection Symmetry" International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013 Procedia Technology 10 (2013) 112 – 120.
9. Pria Bharti, Roopali Soni ,"A New Approach of Data Hiding in Images using Cryptography and Steganography" International Journal of Computer Applications (0975 – 8887) Volume 58– No.18, November 2012.
10. Reyam Jassim Essa*, Nada A.Z. Abdullah, Rawaa Dawoud AL-Dabbagh,"Steganography Technique using Genetic Algorithm" Iraqi Journal of Science, 2018, Vol. 59, No.3A, pp: 1312-1325.

AUTHORS PROFILE

JANANI SUNDAR is Assistant Professor at the department of Computer Science and Engineering in St.Joseph's College of Engineering,OMR, Chennai, India. She received her BE and ME degrees with distinction in Computer Science and Engineering from Anna University Chennai in the year 2009 and 2011. Her current research interests include Machine Learning, Cryptography, Network security, Networks and Web Intelligence.

SHALINI M is working as an Assistant Professor at the department of Computer Science and Engineering in St. Joseph's College of Engineering, OMR, Chennai, India. She completed her BE degree in Computer Science and Engineering from Anna University in the year 2006 and ME degree in Computer Science and Engineering in Sathyabama University in 2011.She currently pursuing her Ph.D in Big data Analytics. . Her current research interests include Machine Learning, Big Data Analytics, Image Processing

Parkavi Murphy John is Assistant professor at the department of CSE in St.Joseph's College Of Engineering,Chennai.she received her B.E. degree in Information Technology in Bharathidasan University, India in 2004, and received her M.E. degree in Computer Science and Engineering, Guidy, Anna University, Chennai, India in 2008. She completed her Ph.D degree in Computer Science and Engineering in the Anna University, Chennai. and her research area includes Wireless communication networks, Modeling and simulation, Soft Computing, Neural Networks, Fuzzy Systems, AI, Sensor Networks, cryptography and network security.

A. Chandrasekar is Professor and Head of the Department of CSE at St. Joseph's College of Engineering, Chennai, Tamil Nadu. He has overall teaching experience of over 21 years in Engineering Colleges. He has guided more than 12 Research Scholars and more than 50 M.E. students. He has published over 110 research articles in refereed International and National journals and he is guiding research scholars and M.E. students in the areas of Network Security, Cloud Security, Data mining, Artificial Intelligence and Big Data Analysis.