ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Image Processing Security Using Secured Hash Algorithm and Kekre's Fast Codebook Generation Algorithm

R.Ramya[1], M.Kavitha[2], S.Hemavathi[3], T.Keerthana[4]

Assistant Professor, Department of Computer Engineering, A.V.C College of Engineering ,Mayiladuthurai, TamilNadu, India[1&2]

P.G. Student, Department of Computer Engineering, A.V.C College of Engineering ,Mayiladuthurai, TamilNadu, India[3&4].

ABSTRACT: The emerging internet technology has led to the need of high level security of data during its transmission. In this paper we fully focused on protect the image processing by using suitable encryption and decryption algorithm. There is some message and a image that has to be sent over the network. In the first phase of Encryption the actual text is converted into another form (cipher text) using SHA 512 algorithm. In the second phase the cipher text is embedded into any part of the image that is to be sent over to the other phase. In the third phase of steganography part the output image of embedding phase is to be taken. Then the phases are to be overlapped at the receiver end and the images are stitched together using KNN algorithm. The receiver end performs the decryption of hiding and embedding phase. The SURF technique is used to improve the quality of image.

KEYWORDS: SHA,KNN,SURF.

I. INTRODUCTION

In today's world of growing technology security is of utmost concern. With the increase in cybercrime, providing only network security is not sufficient. Security provided to images like blueprint of company projects, secret images of concern to the army or of company's interest, using image steganography and stitching is beneficial. As the text message is encrypted using SHA 512 algorithm and embedded in a part of the image the text message is difficult to find. More over since the secret image is broken down into parts and then sent to the receiver. This makes it difficult for the trespasers to get access to all the parts of the images at once. Thus increasing the security to a much needed higher level. This makes it becomes highly difficult for the intruder to detect the and decode the document. There is no limitation on the image format that can be used right from .bmp to a .gif image can be used. It can be grey scale or colored images. The size of the message needs to be of only 140 characters. The work in this paper is divided in two stages. 1) Text- Detection 2) Inpainting. Text detection is done by applying morphological open-close and close-open filters and combines the images. Thereafter, gradient is applied to detect the edges followed by thresholding and morphological dilation, erosion operation. Then, connected component labelling is performed to label each object separately. Finally, the set of selection criteria is applied to filter out non text regions. After text detection, text inpainting is accomplished by using exemplar based In painting algorithm.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

II. RELATED WORK

Current picture of the world says that everything that can be thought off can be done with the help of the internet. Right from shopping for clothes to buying a house. The transactions are all done using personal information, credit card numbers etc. With the amount of internet users hiking day by day, everything that is transmitted over the internet is under threat by some malicious mischief of another person. In order to provide security to the data that is being send across the system network security is not enough. With the growing technology the hackers have also kept themselves updated with technology and ways to hack it. In order to provide security the only way would be not letting the hackers know about the presence of important information in your transaction. Many techniques have been developed to do so like digital watermarking, visual cryptography were used before image steganography. Researchers have also developed techniques that embed data or another image within the image

III. EXISTING SYSTEMS

Various systems are available for information hiding in an image, but they have some drawbacks i.e., they either do not encrypt the message or use a very weak algorithm in order to perform cryptography. They use the same key for encryption and decryption making it easy for the intruder to get access of the information. For example AES algorithm, an encryption algorithm, used keys of smaller sizes (128 bit key) hence it was easy to decode it using computations. Algorithms using keys of these sizes are easily cracked by any intruder. So it is better if one goes for algorithms using keys of larger size which are difficult to decrypt and provide better security. Where stitching is concerned, multiband blending, gain compensation, automatic straightening makes the image
smooth and more realistic.

IV. PROPOSED SYSTEMS

The proposed system is divided into phases for better understanding. The phases are as follow Breaking an image of size w * h into n sub-images of size x * y can be done using blkproc function in matlab.

1. ENCRYPTING PHASE

Secure Hashing Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. A few algorithms of interest are SHA-1, SHA-2, and SHA-5, each of which was successively designed with increasingly stronger encryption in response to hacker attacks. SHA-0, for instance, is now obsolete due to the widely exposed vulnerabilities.

A common application of SHA is to encrypting passwords, as the server side only needs to keep track of specific user's hash value, rather than the actual password. This is helpful in case an attacker hacks the database, as they will only find the hashed functions and not the actual passwords, so if they were to input the hashed value as a password, the hash function will convert it into another string and subsequently deny access. Additionally, SHA exhibit the avalanche effect, where the modification of very few letters being encrypted cause a big change in output; or conversely, drastically different strings produce similar hash values. This effect causes hash values to not give any information regarding the input string, such as its original length..

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

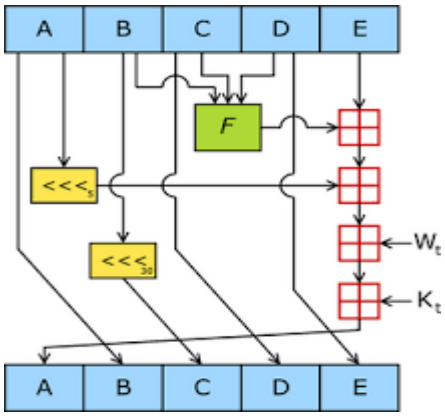

FIGURE 1 :SHA ALGORITHM

In addition, SHAs are also used to detect the tampering of data by attackers, where if a text file is slightly changed and barely noticeable, the modified file's hash value will be different than the original file's hash value, and the tampering will be rather noticeable.

2.EMBEDDING PHASE

In this phase the encrypted message is embedded on to a part of the secret image. In this phase the cipher text that is given as input in the text editor is actually hidden in the cipher.

The LSB steganographic algorithm is used for hiding the cipher inside the image. In this each bit of the cipher text (that has been converted its binary equivalent) is exchanged with the last bit of each pixel value. Similarly for each pixel the last bit is replaced with the consecutive bits of the cipher text i.e. its binary equivalent. Therefore four possibilities of swapping are

ıA '0' replaced by a '0'
ıA '0' replaced by a '1'
ıA '1' replaced by a '0'
ıA '1' replaced by a '1'

So in cases two and three, only the last bit is going to be changed. So the difference in the resulting pixel value is not going to show much difference. Hence the resulting image will reassemble the original image. This technique of replacing the bits is called the LSB technique in steganography. The LSB technique together with the masking technique provides more security. Masking is nothing but replacing the bits in the pixel before, the binary equivalent of the character is binary ANDed with 254.

3.HIDING PHASE

In this phase image steganography is performed. The technique used for image steganography is (KFCG) .KFCG does not use Euclidean distance to generate the codebook. Let T is the initial training vector. T contains m training vectors each of size k. T= {X1, X2,..., Xm} and X1= {x11,x12,…….x1k}. Initial code vector C1 is computed as centroid of training vector T.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

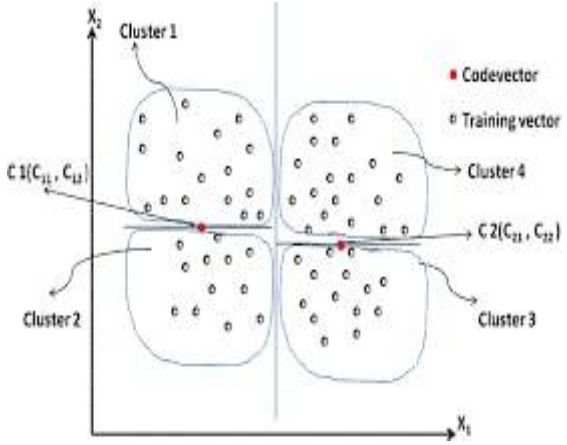

FIGURE 2:KFCA FOR TWO DIMENSION

In first iteration, first element of each training vector of T is compared with the first element of code vector. i.e. if xi1< C11 then put Xi in cluster 1 else in cluster 2. In second iteration, split cluster1 into two by comparing xi2 with second element of the centroid of cluster 1 and cluster 2 into two by comparing xi2 with second element of the centroid of cluster 2. Repeat this procedure till codebook of desired size is generated.

4.STITCHING PHASE

K-Nearest Neighbour or KNN algorithm is part of supervised learning, it is also a non parametric technique, which means that no assumption is made about the parameters in this algorithm..[1]the working is based on finding the minimum distance from the query instance to the training samples to determine the K-nearest neighbours to the query instance. After we find the k nearest neighbours simple majority of these K-nearest neighbours is taken to be the prediction of the query instance.

ü An arbitrary instance is represented by (a1(x), a2(x), a3(x),.., an(x))
ai(x) denotes features

ü Euclidean distance between two instances
d(xi, xj)=sqrt (sum for r=1 to n (ar(xi) - ar(xj))2)

Algorithm: Automatic Panorama Stitching

Input: n unordered images

I. Extract SURF features from all n images

II. For each feature find nearest- k -neighbours using a k-d tree

III. For each image:

(i) Select m candidate matching images that have the most feature matches to this image

(ii) Use RANSAC to find geometrically consistent feature matches to solve for the homography between pairs of images

(iii) Using a probabilistic model verify image matches

(iv) Find connected components of image matches

(v) For each connected component:

(vi) Perform bundle adjustment to solve for the rotation _1, _2, _3 and focal length f of all cameras

(vii) Render panorama using multi-band blending

Output: Panoramic image(s)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

V.CONCLUSION

This paper has presented a novel system for data and image encryption using SHA algorithm for cryptography, image steganography and image stitching which can be used by banking, consultancies and detective agencies. It has put forth a new system which combines text cryptography and image Steganography which could be proven a highly secured method for data transactions in the near future. As the image to be sent is broken down into parts and encrypted individually and sent over the network it becomes difficult of the intruder to get access of all the parts. With the help of SURF features and RANSAC algorithm the output of the image is rectified and we get a smooth image. This image can also be used as a password to open a document of a file.

REFERENCES

[1] Matthew Brown and David G.Lowe ”Automatic Panoramic Image Stitching using Invariant Features”, Computer Science, University of British Columbia, Vancouver, Canada
[2] H. B. Kekre, Tanuja K. Sarode ”High payload using mixed codebooks of Vector Quantization”, ArchanaAthawale, KalpanaSagvekar
[3] Dr. H.B. Kekre, ArchanaAthawale, TanujaSarode, SudeepThepade&KalpanaSagvekar ”Steganography Using Dictionary Sort on Vector Quantized Codebook”, International Journal of Computer Science and Security (IJCSS), Volume (4): Issue (4) 392
[4] H.B.Kekre,ArchanaAthawale and Pallavi N.Halarnkar, ”Polynomial Transformation to improve Capacity of Cover Image For Information Hiding in Multiple LSBs”, International Journal of Engineering Research and Industrial Applications(IJERIA),Ascent Publications, Volume 2,March 2009,Pune.
[5] H.B.Kekre,ArchanaAthawale and Pallavi N.Halarnkar, ”Performance Evaluation of Pixel Value Differencing and Kekre’s Modified Algorithm for Image Hiding in Images”,ACM International Conference on Advances in Computing, Communication and Control(ICAC3)2009.
[6] Dipti Kapoor Sarmah1 and Neha Bajpai2 ’Proposed System for data hiding using Cryptography and Steganography * Department of Information Technology, Center of Development of advance computing,Noida, INDIA.
[7] D. Lowe “Distinctive image features from scale-invariant keypoints. International Journal of Computer Vision, 60(2):91–110, 2004.
[8] H. Seetzen, W. Heidrich, W. Stuerzlinger, G. Ward, L. Whitehead, M. Trentacoste, A. Ghosh, and A. Vorozcovs, “High dynamic range display systems”. In ACM Transactions on Graphics (SIGGRAPH’04), 2004..
[9] R. Szeliski, “Image alignment and stitching” A tutorial. Technical Report MSR-TR-2004-92, Microsoft Research, December 2004.
[10] P. Torr, “Bayesian model estimation and selection for epipolar geometry and generic manifold fitting” International Journal of Computer Vision, 50(1):35–61, 2002.
[11] J. Sivic and A. Zisserman. Video Google, “A text retrieval approach to object matching in videos” In Proceedings of the 9th International Conference on Computer Vision (ICCV03), October 2003.
[12] P. Debevec and J. Malik, “Recovering high dynamic range radiance maps from photographs” Computer Graphics, 31:369–378, 1997.

.