ICITKM
Proceedings of the First International Conference on Information Technology and Knowledge Management pp. 89–92
DOI: 10.15439/2018KM19
ISSN 2300-5963 ACSIS, Vol. 14

An Adaptive Approach for image adaptive watermarking using Elliptical curve cryptography (ECC)

Naveen Kumar [1], Prakarti Triwedi[2], Pramod Singh Rathore [3]

[1]*Computer Science & Engineering, Govt. Engineering College, Ajmer, India*
[2]*Assistant Professor, Computer Science & Engineering, Govt. Engineering College, Ajmer, India*
[3]*Assistant Professor, Computer Science & Engineering, Aryabhatt College of Engg. & Research Center, Ajmer, India*
[1]*naveennarlia @gmail.com,* [2] *niyuvidu@ rediffmail.com,*[3]*pramodrathore88@gmail.com*

***Abstract*—Elliptical curve cryptography (ecc) is a public key encryption approach based on elliptic curve idea that may be used to create quicker, smaller, and greater green cryptographic keys. Ecc generates keys through the houses of the elliptic curve equation in area of the traditional approach of generation as the manufactured from very huge prime numbers. The technology may be used at the side of maximum public key encryption strategies, together with rsa, and diffiehellman. Consistent with some researchers, ecc can yield a degree of safety with a 164-bit key that different structures require a 1,024-bit key to advantage. Because of the fact ecc helps to establish equivalent safety with decrease computing power and battery useful resource usage, it's far turning into widely used for cellular programs.**

In this work we implement ECC Algorithm with altered approach for encrypting and decrypting the probe image and encrypted images respectively. Our proposed approach has proposed that the elapsed time to perform the task for same input image is less than the conventional approach. We have run the cryptography procedure for n number of iterations in order to get the accurate results and compared that particular elapsed time with the conventional approach. We have contemplated an approach in which we consider region of interest (ROI) unlike the conventional approach, the advantage of the proposed work is we n need not to cover all the pixel vectors but only those which is required to be encrypted or decrypted. The proposed work has applied ecc algorithm for error calculations which has been shown in the experimental results. The proposed work has compared the result in both the aspects in terms of elapsed time to perform the algorithm and ROI feature to get implemented at the same time.

***Index Terms*—Object MATLAB, rsa, ECC, cryptographic.**

I. Introduction

IN RECENT years, virtual multimedia generation has proven a significant development. This generation gives so many new blessings as compared to the antique analog counterpart. The advantages throughout the transmission of information, smooth enhancing any part of the digital content material, functionality to duplicate and verbal exchange applications have made the digital technology superior to the analog structures a virtual content without any loss inside the first-class of the content and lots of different blessings in dsp, vlsi. specially, the boom of virtual multimedia generation has proven itself on net and wireless programs. but, the distribution and use of multimedia information is an awful lot simpler.

That it remains present as long as the perceptible first-class of the content cloth is at an appropriate diploma. The owner of the specific information proves his/her ownership with the aid of extracting the watermark from the watermarked content cloth in case of more than one possession claims. Digital watermark can be and faster with the exceptional achievement of net. The first-rate explosion in this period has additionally introduced some troubles beside its advantages. But, abuses of those centers and technology pose urgent threats to multimedia safety management in widespread and multimedia copyright protection and content integrity verification mainly. Despite the fact that cryptography has an extended history of utility to records and multimedia security, the unwanted function of offering no protection to the media as quickly as decrypted has restrained the feasibility of its large use. For instance, an adversary can collect the decryption key by means of buying a legal replica of the media however then redistribute the decrypted copies of the proper .In reaction to those demanding situations, digital watermarking schemes were proposed in the very last decade. A produced from copyright or authentication codes, or a legend important for sign interpretation. The existence of those watermarks with in a multimedia signal goes ignored except while surpassed through the best detector. Commonplace sorts of indicators to watermark are nonetheless photos, audio, and virtual video. Watermark [1], a thriller imperceptible sign, is embedded into the authentic facts in the form of way.

Watermarking is described as adding (embedding) a watermark sign to the host signal. the watermark may be detected or extracted later to make an announcement approximately the object. A general scheme for digital watermarking is given in Figure 1.1. The watermark message can be a logo picture, sometimes a visually recognizable binary picture or it can be binary bit stream. A watermark is embedded to the host data by using a secret key at the embedded.

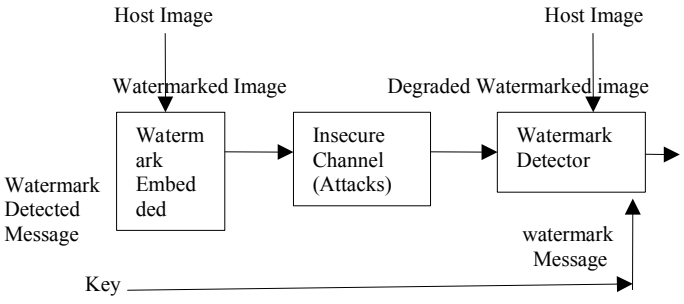

Fig 1: A Digital Watermarking System

II. Overview of Digital Watermarking

Digital watermarking is a prominent discipline of research and lots of researchers have advised a big quantity of algorithms and as compared. The main thrust on all such algorithms is to hide secrete information (watermark) in host signal in such a way that it offers appropriate tradeoff among imperceptibility and robustness against distinct assaults. this segment gives several kinds of virtual watermarking techniques found in the instructional literature. we do now not deliver an exhaustive assessment of the area, however offer an outline of installed approaches. current virtual watermarking techniques are broadly categorized into classes relying at the area of watermark insertion: spatial area and frequency domain techniques.

The sooner watermarking techniques are nearly spatial primarily based completely method. In spatial place the watermark is embedded into the host image by way of manner of using the usage of the usage of without delay improving the pixel values, i.e. First-rate example is to embed the watermark inside the least considerable bits (lsbs) of photo pixels [1]. Spatial area watermarking is simple to position into impact and requires no unique photograph for watermark detection. But, it frequently fails underneath signal processing assaults which consist of filtering and compression and having relative low-bit functionality. A easy photograph cropping operation may also moreover additionally eliminate the watermark. Besides, the constancy of the particular image facts may be significantly degraded because of the truth the watermark is at once finished on the pixel values.

In assessment to the spatial-vicinity-based absolutely watermarking, frequency-location based strategies can embed greater bits of watermark and are extra robust to assault; therefore, they're greater attractive than the spatial-area-based strategies, because the watermark records may be unfold out to the complete image. as to the frequency transform, there are dft (discrete fourier rework), dct (discrete cosine remodel), and dwt (discrete wavelet remodel).

III. Problem Formulation and Proposed Solution

In this work we implement ECC Algorithm with altered approach for encrypting and decrypting the probe image and encrypted images respectively. Our proposed approach has proposed that the elapsed time to perform the task for same input image is less than the conventional approach. We have run the cryptography procedure for n number of iterations in order to get the accurate results and compared that particular elapsed time with the conventional approach. We have contemplated an approach in which we consider region of interest (ROI) unlike the conventional approach, the advantage of the proposed work is we n need not to cover all the pixel vectors but only those which is required to be encrypted or decrypted. The proposed work has applied ecc algorithm for error calculations which has been shown in the experimental results.

Input variables:

Image: the profile desires to be warped to be able to be similar to template,

Template: the profile desires to be reached,

noi: the number of iterations according to level; the set of rules is finished

(noi-1) times

Ranges: the number of ranges in pyramid scheme (set tiers=1 for a non pyramid implementation), the extent-index 1

Corresponds to the very best (authentic) picture resolution

Rework: the image transformation 'translation', 'euclidean', 'affine', 'homography'

Step 1-Take all the input image at the same time

Step2- Apply ROI on the probe image in order to get it in template then the particular segmented region with required pixel information is fetched.

Step3-Projected coordinates are selected as per requirement to reduce the total elapsed time in performing N number of iterations.

Step4-Perform backward wrapped input image so that maximum resolution can be evolved.

Step5-Finally error calculation of that particular image is calculated and shown using conventional ecc.

The above steps are first module of our work; the second module will include the following steps.

Step6-Then –The proposed approach has been applied on image with number of iterations

Step7- The total elapsed time is calculated comparatively, with the conventional approach.

Step8-This approach will result in the final aligned image retrieved from the encrypted image with Roi concept.

Step9-Repeat the above step till the last number of iteration for maximum threshold

Step10- EXIT

IV. RESULT

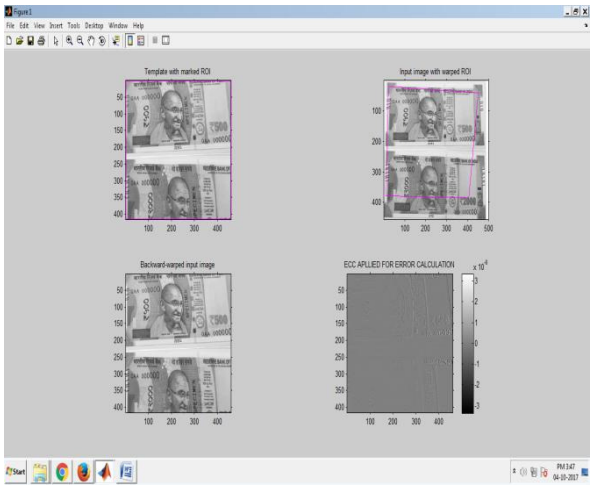

Fig 2- Error Calculation Using Roi Applied Ecc Algorithm

The input image of Indian currency note is template with roi and the second sub plotted image is showing the image with ROI effect .then the image is back wrapped with the final consideration of pixel vectors which comes under the roi segmentation. The final step is the calculation of error while performing cryptography which is clearly shown in the results. The ROI concept has been used along with conventional Ecc algorithm to keep the resolution of image as same as original but considering only those pixel vectors which are required .this make the algorithm time efficient as far as elapsed time is concerned for the execution of the algorithm.

V

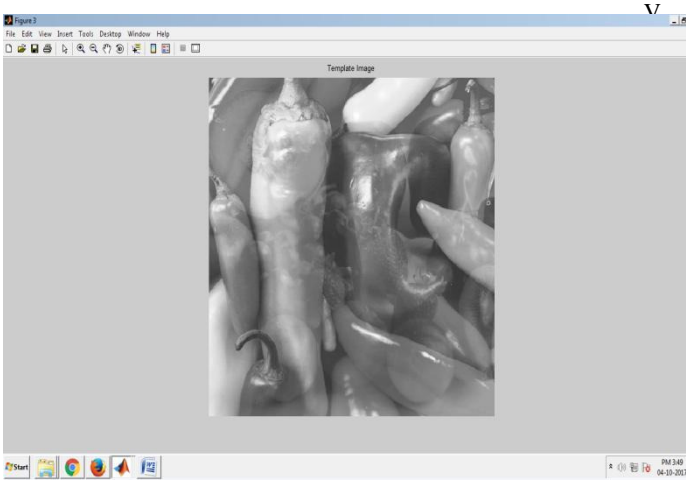

Fig: 3 ROI polygons to interest mask

The comparison in the image between different pixel vectors has been performed in template matching on the basis of correlation coefficient .In this particular process the target image is placed over the initial probe image in such a way that it will create a correlation map on the basis of which final template image is generated.

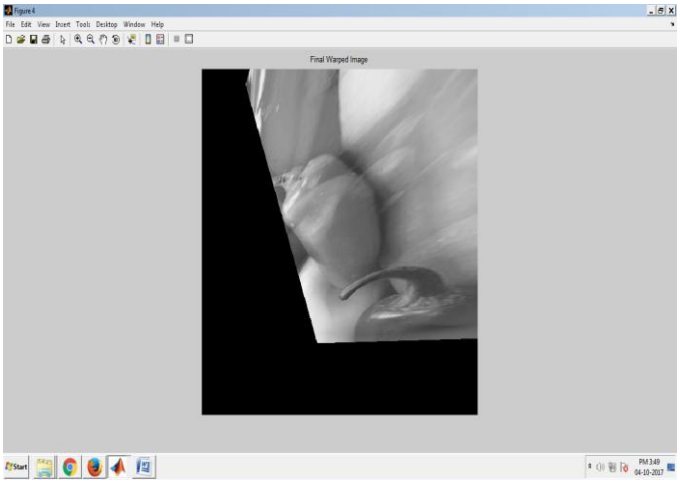

Fig 4: Template matching in the ecc

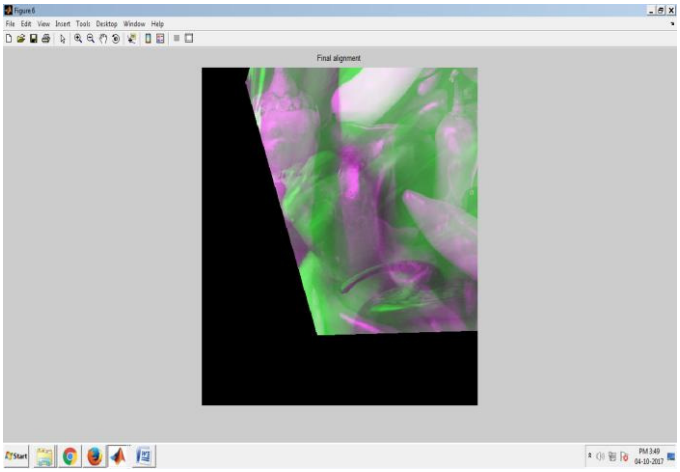

Fig 5: same intensity and resolution as the original image

Image wrapping is a transposition which is finally applied to the image in which template part is generated. It is applied on particular domain of the image in order to modify the geometrical properties in the given image .The image shown above has same intensity and resolution as the original image, We have performed it with Ecc algorithm to perform forward and backward mapping and sampling in spatial dimensions .The main goal of this method to get applied with ecc is to re-sampling the intensity value .the method which are common in use are bilinear cubic nearest neighbour etc. The image shown is performed by bicubic re-sampling of image intensity.

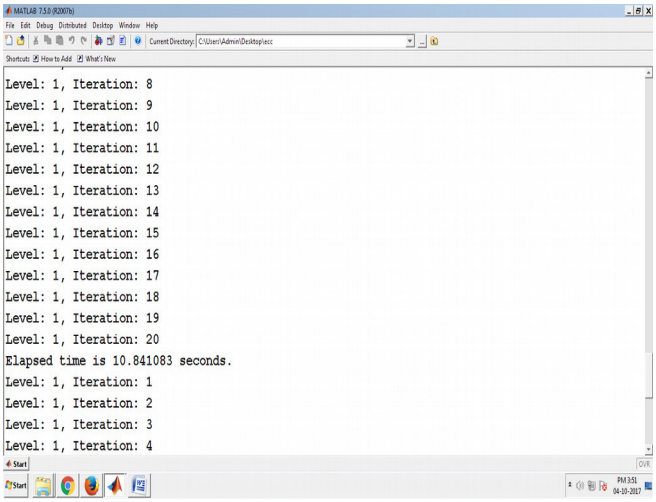

Fig 6: time elapsed in conventional approach and proposed approach

The final result has shown the reduced estimated elapsed time for running the proposed algorithm on specific domain of the image as compare to the conventional approach. . For the level 1we have calculated for 50 number of iteration because we have set the global threshold value in order to make compatibility with memory configuration. The total elapsed time calculated with conventional Ecc algorithm is 21.31 sec depicting in the result section now the proposed algorithm has reduced the complexity of the network by reducing the elapsed time to 10 sec approx at the same time several other methods have been applied to improve the accuracy of the results

IV. Conclusion And Future Work

Within our research, we have characterized and examined tremendous image segmentation calculations. Mage segmented calculations have a promising destiny in advance considering the fact that they're the basis of picture preparing and pc imaginative and prescient and feature was the center of contemporary studies. Notwithstanding quite a few years of research, there may be no generally mentioned set of rules segmentation calculation. Considering the fact that photo segmentation is motivated by way of bunches of additives, as an instance, type of photo, shading, threshold, degree of noise, and so forth. Along those lines there's no single calculation that is pertinent on a extensive range of pictures and nature of issue. Because of each single above detail, photograph segmentation still stays a primary pending trouble in the tiers of photo preparing.

In gift method we had labored on a static picture, in future the work may be finished on a moving image (video)

References

[1] Stenger, A., Rabenstein, R.: Adaptive Volterra Filters For Nonlinear Acoustic Echo Cancellation. In: Proc. NSIP, vol. 2, pp. 679–683 (1999)

[2] 4. Paleologu, C., Benesty, J., Ciochin, S.: A Variable Step-Size Affine Projection Algorithm Designed for Acoustic Echo Cancellation. IEEE Transactions on Audio, Speech, and Language Processing 16, 1466–1478 (2008)

[3] Van Schyndel, R. G., Tirkel, A. Z., and Osborne, C. F., “A digital Watermark.” Proc. of the IEEE Int. Conference on Image Processing. Vol. 2, (1994): pp. 86-90.

[4] Swanson, M.D., Kobayashi, M., and Tewfik, A.H., “Multimedia Data-Embedding and Watermarking Technologies.” Proc. of the IEEE. Vol. 86, No. 6, (June 1998): pp. 1064– 1087.

[5] Petitcolas, F., Anderson, R., and Kuhn, M., “Information Hiding—a Survey.” Proc. of the IEEE. Vol. 87, No. 7, (July 2016): pp. 1062–1078.

[6] Barni, M., Bartolini, F., Cox, I.J., Hernandez, J., and Perez-Gonzalez, F., “Digital Watermarking for Copyright Protection: A communications perspective.” IEEE Communications Magazine. Vol. 39, No. 8, (August 2015):pp. 90–133.

[7] Langelaar, Gerhard C., Setyawan, I., and Lagendijk, R. L., “Watermarking Digital Image and Video Data: A state-of-the-art-overview.” IEEE Signal Processing Magazine. Vol. 17, No. 5, (September 2015): pp. 20-47.

[8] Voyatzis, G., Mikolaides, N., and Pitas, I., “Digital watermarking: An overview.” Proc. of IX European Signal Processing Conference(EUSIPCO), Island of Rhodes, Greece. (September 8-11, 2014): pp. 13-16.

[9] Wolfgang, R. B., Podilchuk, C. I., and Edward J. Delp, “Perceptual Watermarks for Image and Video.” Proc. of the IEEE. Vol. 87, No. 7, (July 2013): pp. 1109-1126.

[10] Cox, I. J., Miller, M. L., and Bloom, J. A., “Watermarking Applications and their Properties.” Proc. of IEEE Int. Conference on Information Technology, Las Vegas. (March 2012): pp. 6-10.

[11] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M. M., “Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications.” IEEE Journal On Selected Areas in Communications. Vol. 16, No. 4, (May 1998): pp. 573-586

[12] Ruanaidh, J. J. K. O’, and Pun, T., “Rotation, Scale and Translation Invariant Digital Image Watermarking.” Proc. of IEEE Int. Conference on Image Processing, Santa Barbara, CA, USA. Vol. 1, (October 2011): pp. 536-539.

[13] Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T., “Secure Spread Spectrum Watermarking for Multimedia.” Proc. of IEEE Int. Conference on Image Processing. Vol. 6, (December 2011): pp. 1673-1687.

[14] Boland, F. M., Ruanaidh, J. J. K. O’, and Dautzenberg, C. “Watermarking Digital Images for Copyright Protection.” Proc. of IEEE Int. Conference on Image Processing and its Application, Edinburgh, U.K. (July 2009): pp. 321-326.

[15] Barni, M., Bartolini, F., Cappellini, V., and Piva, A., “A DCT Domain System for Robust Image Watermarking.” Signal Processing Archive. Vol. 66, No. 3, (May 2008): pp. 357- 372.