ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Hybrid Algorithm using Color Image Visual Cryptography, Vector Stegnography and Random Key Cryptography for Digital Image, E-Stamp and Digital Signature Authentication

Pratibha Gupta
Dept. of Digital Communication
Yagyavalkya Institute of Technology, (YIT)
Jaipur, India

Amit Sharma
Asst. prof. of Electronics and Communication
Yagyavalkya Institute of Technology,(YIT)
Jaipur, India

Abstract: Digital documents play a major role in modern era. They are cost to create, modify and manage. The easy modification of digital document makes them more valuable and prone to forgery. Digital documents can easily to tampered and forged. Advances in information technology, e-commerce and e-governance activities pose on immediate challenge to produce digital document that are highly resistant to forgery and are and highly reliable in confirmation of owner detail. In this Endeavour we propose a hybrid system comprised of color image visual cryptography, vector stegonography (water marking) and truly random key cryptography to achieve highly reliable authentication of digital image, e-stamp and digital signature.

Visual cryptography is a special encryption technique to divide information is share image in such a way that it can be decrypted by the human eye or human vision system (HVS). Stegenography (is the act of hiding a message related for digital signal such as an image or video etc. Within another image, video or another digital content. Cryptography is a method for storage and transmission of data in a particular form that only those for whom it is intended can be discribe or process it. We have combined those above three techniques to achieve digital image authentication.

Keywords: Color Visual Cryptography, Vector Stegnography, Truly Random Key Cryptography, Image Processing, MATLAB.

I. INTRODUCTION

Visual Cryptography (VC) is a way to encrypt a secret image in a shared way to stack a sufficient number of secret shared screen images. The stock is a binary image that usually appears in transparencies. Each participant has transparency (share). Unlike traditional encryption methods, VC does not require complex calculations to recover passwords. The decrypted behavior is simply to stack the shared image and see the secret image that appears in the stack share.

Visual encryption technology is a new encryption technology used to protect images. In visual ciphering, images are divided into parts that are called shared and then distributed to participants. The decrypted side only stacks the shared image to get the image [1]. A visual cipher scheme is a concept that encrypts a secret image in n (more than one) shared. Visual coding encodes the secret binary image (SI) in random binary mode. Visual coding encodes the secret binary image (SI) in random binary mode The name of the original image containing the watermark pattern is "image mark" and the watermark image method satisfies transparency and robustness. In this system, we handle color images. We are taking a secret, and the secret is divided into different parts, and then use the DCT algorithm with a secret image for the watermark. After that, we will do n shares the watermark image and then assign n participants. K participants will share the secret with the distributor. This action will find the watermark stored in the database. Then, superimposing these k packets, we will get the image of watermark generated. Then we will apply the inverse DCT in the watermark image to check if the part is valid. If the watermark does not match the database, the participant crashes. If there is not a liar participant, reconstruct the secret. The application will be used for high security areas such as military applications, government applications for authentication [2].

A watermark is a technique in which a secret image is embedded in an overlay image without affecting its perceived quality, so that a secret image can be revealed by some process. A significant advantage of the watermark is the inseparability of watermarks (secret images) and cover images. Some of the important characteristics of the watermark are: difficult to detect, resist common distortions, withstand malicious attacks, transport innumerable fragments of information, coexist with other watermarks, and require little computation to insert and extract watermarks. Generally, a powerful watermark is used to resist malicious or malicious attacks such as scaling, clipping, lossy compression, etc. Watermarking techniques can be classified into different types according to a variety of forms.

Based on the requirements of the extraction or detection of the watermark, the watermark can be divided into non-blind, semi-blind and blind programs. The non-blind watermark scheme requires the original image and secret key for watermark detection. The semi-blind program requires a secret key and a watermark bit sequence to be extracted, while the blind scheme requires only a secret key for extraction. Another classification of watermarks based on embedded data (watermark) is: visible and invisible [3]. The secondary image (watermark) is embedded in the main image through the visible watermark of the image so that the human observer can perceive that the data embedded in the invisible watermark are undetectable; However, it can be detected by a computer program to extract.

Here we propose a program that will increase visual encryption and the benefits of stealth and blind watermarking techniques, use the basic visual encryption model to generate a secret part and then use the invisible and blind watermark to share these watermarks in Some host images. As a result, secret actions are protected against fraud. Decryption will be the same as the visual encryption mode, that is, through the simple watermark extraction technology to extract the secret actions after the stock pile. The proposed watermark scheme does not require the original image or any of its features to extract the watermark, so the proposed scheme is blind. Experimental results have been shown for the efficacy of the invisible and blind watermarking schemes proposed for binary images [4].

II. LITERATURE REVIEW

Gaurangkumar Panchal and others show in the article that To force privacy of data, it is important that an attacker does not have access to resources. There are reports confirming this mechanism. This entire mechanism uses a private key as a password or password key for data encryption. The problem with this technology is the owner must remember the key or store the encryption key of the database, in effect, threatens the system. In this in this paper, we They have solved this problem and have proposed a biometric data encryption strategy to protect the user's own data. It captures the biometric data of the user extracted from it. Then use these function vectors to generate an encryption key. We use the data of this encrypted user, the encryption key follows a process of similar decryption data. We have performed several experiments using a database of standard fingerprint images [5, 6]. The experimental results confirmed that on average 97.25% the user generated the same irrevocable encryption key. The advantage of our method is that it produces unique and key encryption based on dynamic biometrics, storing templates and keys are not required, and faster in terms of key generation is accurate. It is very difficult to generate randomness in cryptography. In cryptography, randomness provides better security. This method is created each time based on different impressions of keys captured from the scanner. The proposed methods the same biometric encryption key can be obtained in our paper fingerprints captured from different scanners are of different image quality.

Rohit Neelam and others stated that the world is totally technology-based. Everyone is addicted to technology and hope that their work becomes a short period of time to complete. No one wants to wait for the message to be sent, and everyone wants to work on their fingertips. Speed and safety are important criteria for this world. So this article is based on the system tdes encrypt and decrypt data. This article improves the speed of the tdes system and the results are compared with the previous tdes result. This article has achieved very good results in this sense of speed. As the speed of tdes increased greatly tdes is working because the speed of encryption and decryption is improved and reinforced. The speed is calculated as 119.5 MHz the internal clock is 500 MHz and the internal clock of 50 MHz is 11.9 MHz clock. This article is based on the encryption and decryption standards of the technology. The proposed tdes implementation provides high-speed performance with very compact hardware. This work was done in the software quartus-ii 8.0 of alter and was implemented in the suites fpga of cyclone-ii. The programming language used in the system is vhdl high level language we get the result is fabulous speed id adds a lot of factors. As you increase speed tdes is more effective than ever. The speed is getting faster the internal clock at 500 MHz is 119.5 MHz and 11.9 MHz at 50 MHz internal clock [7].

Teddy Mantoro et al described in the article that any certification system means providing one's system security. Protecting confidential information Mobile platforms have become a typical trouble-shooting expert. One of the authentication techniques is the text-based password. This type of text password is usually the following, an encryption algorithm that Provides security. This technology has some limitations and drawbacks. When the user chooses to be significant in the dictionary, using violent attacks, it makes the text password susceptible to dictionary and easy to break. To overcome shortcomings, a new certification technique is proposed in this document in order to provide more security authentication system in this article; The text password will be using hiding techniques to hide in the picture. All data and key information (such as passwords) are stored in encrypted use of images as a carrier; It is difficult for violence to crack attack. Steganography is used to hide secret information about a carrier. The most basic and most important image of steganography is embedded bit less significant (lsb) technology. In this technique, the data can be hidden the cover image and the least significant bit of the human eye you will not be able to notice hidden images in the cover file. Lsb steganography and aes encryption technology combined to hide the text password to provide advanced security authentication system running under Android. Stegano-image as a digital key login password in the authentication system mechanism ensures a reliable comparison of other text authentication mechanisms. By using stegano-image, you can make any system more secure this will be conducive to cooperation from the world of application, government and individual use. Algorithm eliminate strong attacks. All data and key information. If the password is stored in encrypted mode embedded in a cover image, so it is difficult to attack attack violence. Finally stegano-image is secure authentication system provides advanced security system contains most important data, especially in the mobile computing environment [8].

Bias sekar avi shena et al described that the use of digital images has increased the integrity of today and the image becomes an important one should prevent any aspect of the attack. Image protection should not change the image content and is also sensitive to changes caused by third-party intentional attack) is robust for incidental attacks such as noise. The multimedia signature scheme (mss) is one of several plans used to protect the integrity of the image. The program uses the image function to generate an image signature. Certification

The process is done by comparing the features extracted from the signature and receiving the image function. This article uses a combination of mss and feature extraction called second order function statistics to create a high quality image and image integrity protection certification program. The signature of the image will incorporate watermark technology to introduce the image. There is watermark the program produces better image quality to the original image. Experimental results show efficacy where detection accuracy is close to 74.2%. The authentication scheme based on second-order feature statistics performs well on imperceptibility, robustness and sensitivity. Robustness and precision sensitivity Respectively, 64.7% and 87.25%. And detection accuracy Reaching 74.2%. False positivity rate of robustness, sensitivity and certification process near 38.8% 1% and 35.5%, respectively. These results indicate that the proposed program can accurately identify false and real images. Even if there are some weaknesses, such as recognition, the image is flipped and the added white Gaussian noise is attacked. In addition, the program produced a good watermark Of which 81 images meet the standard PSNR images: 40 dB [9].

III. METHODOLOGY

Implementation of Visual Cryptography when Information is in Image Form When the image form exists, it is easy to achieve visual cryptography to protect the data. In visual ciphering, if the information is in the form of an image, it does not work this way. Each pixel in the image is divided into smaller blocks. It always has the same number of white (transparent) and black blocks. If the pixels are divided into two parts, there is a white and a black block. If the pixels are divided into four equal parts, there are two white and two black blocks.

The example image above uses pixels divided into four parts. In the figure we can see that a pixel is divided into four parts, there can be six different states. If the pixels in layer 1 have a given state, the pixels in layer 2 can have one of two states that are the same or reversible with the pixels in layer 1. If the pixels in layer 2 are the same as layer 1 , The pixels to be covered will be half black and half white. This superimposed pixel is called gray or white. If the pixels in layers 1 and 2 are inverted or inverted, the covered version will be completely black. This is an information pixel. Now we can create two layers. A transparent image (layer 1) has all the pixels with a random state, one of six possible states. Layer 2 is the same as layer 1, except that the overlapping pixels must be black (containing information). These pixels have an opposite state to the same pixel in layer 1. If the two images overlap, the regions with the same state will appear in gray and the area with the opposite state will be black. Pixel systems can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangular blocks, or even split circles. Also, the pixels are horizontal or the vertical segmentation is not important [10].

There are many different pixel systems, some with better contrast, higher resolution or even with color pixels. Pixel size or color and resolution can be used as required by the condition or problem. In figure 3, the result is given 12, but the overlap or combination of empty pixels and information pixels can be done in several ways. If the pixel status of layer 1 is true (secure encryption), the blank elements of layer 2 and the information pixels will also have a completely random state. It is not possible to know if the pixels in layer 2 are used to create gray or black pixels because we need the pixel state in layer 1 (which is random) to know the results of the overlap. If it meets all the requirements of true randomness, visual cryptography provides absolute confidentiality based on information theory.

If you use visual cryptography for secure communication, the sender will distribute one or more random layers 1 to the receiver. If the sender has a message, create a layer 2 for the particular distribution layer 1 and send it to the receiver. The receiver is aligned with the two layers and displays the secret information, which does not require an encryption device, a computer or a manual execution of the calculation. The system is not destructive, as long as the two layers do not fall into the wrong hands. When one of the two layers is intercepted, it is not possible to retrieve the encrypted information.

Color Modal

The image fingerprint image is a method in which information related to the image and its owner may be hidden in the image (cover image) itself. The unique image ID, customer ID, and name of the image will be used as the fingerprint for each image sales transaction. The unique fingerprint will be embedded in the particular image. A text-to-image conversion algorithm to prepare the secret data will be used to generate the fingerprint. The novelty of the algorithm lies in the method of fingerprint recognition. It is visually encrypted for improved security. Fingerprints are divided into parts of the same size, and do not contain any important information about fingerprints alone, unless they visually overlap.

The complete information in the fingerprint is evenly distributed among all actions. It is visually encrypted for improved security. Fingerprints are divided into parts of the same size

It does not contain any important information about the fingerprint, unless they are superimposed on the visual. The complete information in the fingerprint is evenly distributed among all actions. In order to serve the purpose of fingerprint identification, the images embedded in different blocks embedded in the frequency domain are shared. A single cover image will contain all parts of the fingerprint. Even a part of the fingerprint is detected, but does not detect each part successfully, it is impossible to regenerate the fingerprint. So there are no illegal people who can not know all the actions in the case of fingerprints.

Our Implementation In Color Visual Cryptography

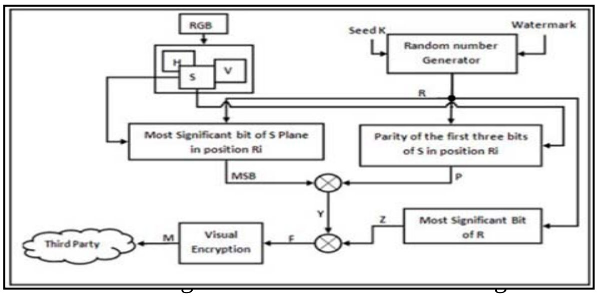
First we start then do Input binary image for visual cryptography, then create share matrix share 1 & share 2. Then do initialize matrix S1a & S2b. Then find coordinates of pixels corresponding to while or in input image. Then do initilize i (loop control) to 1. Then do Share 1 and Share 2. Then do Increment i by 1. Then we check i = len (x), If Yes then Display Initilize Soa = [1 0] & Sob = [0 1]. Else turn to Initilize i. And Display Initilize Soa & Sob then find coordinates of pixels corresponding to block or 0 in Input Image. Then do Initilize i (loop control) to 1. Then do a = X(i) and b = Y(i) Generate Random Share using control Soa & Sob. Then do Share 1(a) and Share 2(a). Then do Increment i by 1. Then check i = len(x). If Yes then do Share 12 = Bitor & Share 12 = Compliment display. Else turn to Initilize i(loop control). And Share 12 then flowchart has goes to End.

Watermarking

As can be seen from Figure 2, the size of the new image will be twice the original size. It has been studied to make the technique useful for grayscale images and color images [Macpherson, 2000, Wang et al. 2003, Shyu 2006]. Tuyles et al. Have tried the decryption scheme based on XOR operations [Tuyls et al 2005]. Lee et al. An interference encryption technique using XOR operation is proposed [Lee et al 2002]. Experiments have been carried out on color images that have been expanded for visual encryption schemes. Vietnam and Black pool try to use the NOT operation to improve the quality of reconstructed images [Viet, Korosawa 2004]. The XOR operation has been implemented by a function reversal.

Although the conventional plan produces meaningless shares, but meaningful shares have also been expanded Visual Encryption Program When the stock is superimposed, these meaningful stocks disappear, the original secret recovery

[Naor, Shamir 1996]. In addition to the adverse effects on contrast and image resolution, the visual cryptographic scheme has been found to be heavily dependent on user authentication. It uses the traditional (k, n) scheme, and the number of sub pixels is 1. The structure of the scheme is defined by the Boolean vector, which is based on the color of the pixels in the various shares


RGB
H
S
V
Seed K
Watermark
Random number Generator
R
Most Significant bit of S Plane in position Ri
Parity of the first three bits of S in position Ri
MSB
P
Y
Z
Most Significant Bit of R
Third Party
M
Visual Encryption
F

Truly Random Key TRK – Cryptography

The extraction algorithm extracts the watermark from the intensity image of the main image in the case of the gray scale or the Y component of the color image. The relevant component of the host image is called the watermark image O. In the preprocessing phase of the algorithm, an image is obtained to obtain the desired component decomposition. The other inputs of the algorithm are the main shared M and the secret key K. The output of the extraction algorithm is the extracted watermark S '. Figure 2.B shows the process of extracting a watermark from a watermarked image. As can be seen from the figure, the extraction algorithm follows the same process as the embedding algorithm to create a binary matrix Y with a size of wxh. In this way, the guaranteed shared V of wx2h is created so that if the elements in the binary matrix Yi are "0", then allocate Vi = (0,1) otherwise allocate Vi = (1, 0). Finally, you can extract the watermark by performing bitwise logic or operations on the primary and authentication shares [11].

IV. Result

We have taken sample images Lena256 and Carey as original images, with respective resolution 256*256 and 221*373 and respective size(s) 15.8kb and 21.1kb.

Table 4: Specifications of Original Image

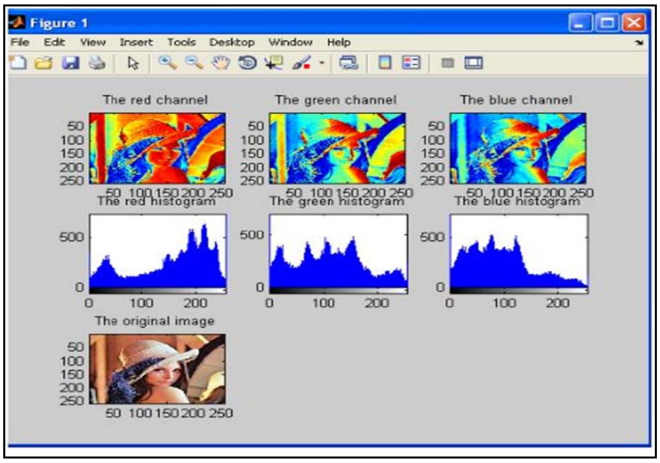
S.NO	Name of image	Resolution	Size of image
1.	Lena256	256*256	15.8 Kb
2.	Carey	221*373	21.1 Kb

Figure 2: Sample Image Lena 256

Figure 3: Sample Image Carey

Color Analysis Of Original Image

As shown previous topic, we take two original images Lena256 and Carey. With responsive resolution 256*256 and 221*373 and responsive size 15.8kb and 21.1kb.We have processed color analysis of each images with each cover images. And we found result as below



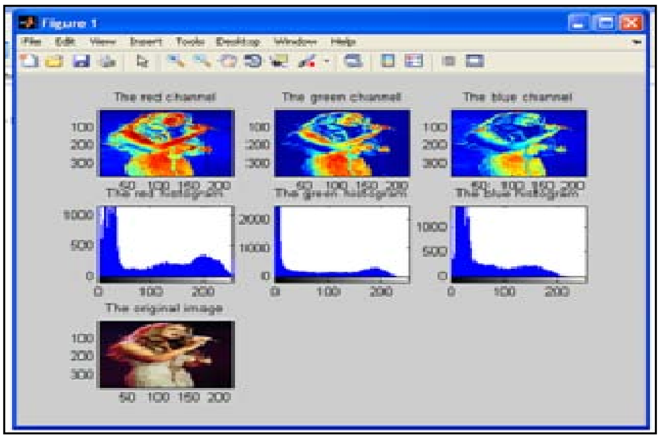


Figure 6: Image Color Analysis Of Carey

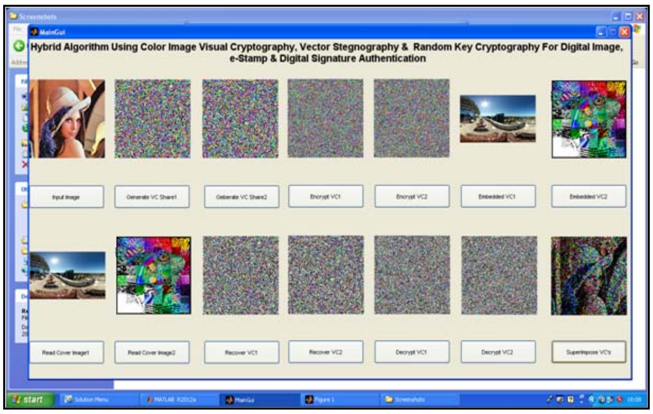
Table 7: Image Color Analysis Of Original Images

S.No	Name	Red Standard Deviation	Red Color Value	Green Standard Deviation	Green Color Value	Blue Standard Deviation	Blue Color Value
1	Lena256	1074.33	32	775.21	32	1095.80	32
2	Carey	1929.33	32	5526.22	8	2801.16	24

In process flow, we encrypted the below images with given two cover images. In this process, we have two original images (Lena256 and Carey) to encrypt with each cover images.

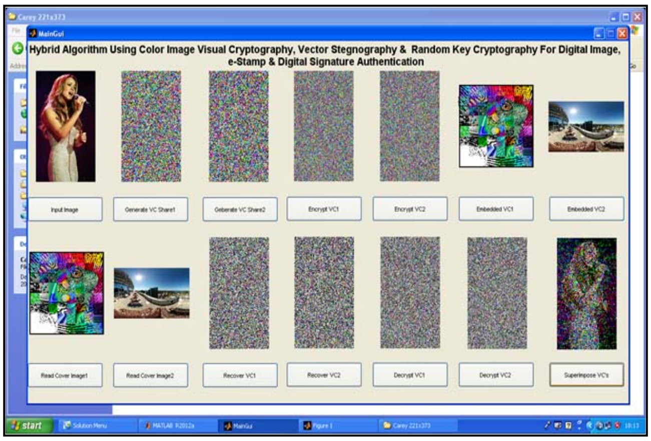
First we took Lena256 to encrypt with cover images (Pano and Frymire). After that the image generate in VC share1 and VC share 2. that these images, they encrypted in Encrypt VC1 and Encrypt VC2. And than they embedded with each cover images. And found Embedded VC1 and Embedded VC2. And to recover this image, we took both cover image Read Cover Image 1 and Read Cover Image2.

Then recovered in Recover VC1 and Recover VC2. After the decryption of these, (Decrypt 1 and 2) we found superimpose VC's.



Hybrid Algorithm Using Color Image Visual Cryptography, Vector Stegnography & Random Key Cryptography For Digital Image, e-Stamp & Digital Signature Authentication

Figure 8: Process Flow 1



Hybrid Algorithm Using Color Image Visual Cryptography, Vector Stegnography & Random Key Cryptography For Digital Image, e-Stamp & Digital Signature Authentication

Figure 9: Process Flow 2 For Original Image Carey

V. CONCLUSION

Today in the information era, when the world has become a global village, digital document authentication and security has emerged major issues. A unique system comprising hybridization of three distinct image security techniques has been proposed. This system reliably authenticates the ownership of authenitive document and signatures. Authorized personnel (government/any organization issuing the document) can extract the water marked image share using the truly random cryptography key provided. Thus, a malicious parson can't destegnograph/dewater mark and forge the document, since be does not possess a valid secret key. If a document is rescaled or cropped and modified, the changes destabilize the recovery of vector stegenography, and thus render forgery almost impossible. Experimental result conclude that the proposed technique achieves 100% accuracy in authentication of digital documents.

VI. FUTURE SCOPE

As proposed, digital image security and ownership authentication is a promising and challenging field in future online e-commerce and e-governance system. We have proposed a hybrid system to cater to these need but still a lot of advancement is required in authentication technologies to cope up with existing and future threads. One of the major enhancements can be integration of biometric signature with the digital document to ensure cent per cent owner authenticity. Another major scope for be addressed, is the development of new and evolved compression algorithm so that compression does not interfere with digital image authentication techniques. Also future scheme need to concentrate on color visual cryptography schemes which enable less pixel expansion along with maintaining contrast and color balance.

VII REFERENCES

[1] List and number all bibliographical references in 9-point Times, single-spaced, at the end of your paper. When H. M. Rafeed Leon, Md. Asaduzzaman Shoeb, Md. Saifur Rahman, Muaser Uddin Ahmed, and Md. Sadiqul Islam, "Design and economic feasibility analysis of autonomous hybrid energy system for rural Bangladesh," 2016 4th International Conference on the development in the in Renewable Energy Technology (ICDRET), pp. 1-6, 2016.

[2] Akshay B. Zade, Asha Gaikwad, Ku. Prachi M. Jeevane and Ganesh Lohote, "Hybrid Solar and Wind power generation with grid interconnection system for improving power quality," 2016 IEEE 1st International Conference on Power Electronics Intelligent Control and Energy Systems (ICPEICES), pp. 1-6, 2016.

[3] Lini Jacob and Divya S Nair, "Stand alone hybrid power generation-control technique for dump power," 2016 International Conference on Energy Efficient Technologies for Sustainability (ICEETS), pp. 96-100, 2016

[4] Mohammd Reza Maghami, Chandima Gomesh, Hashim Hizam and Mohammad Lutfi bin Othman, "Design of 24 Hour Energy Generation from Renewable Energy," 2015 IEEE European Modelling symposium (EMS), pp. 284-287, 2015.

[5] Aunanna Rashid, Nabil Hasan, Khandokar Tanvir Parvez and Md. Nasimul Islam Maruf, "Study and analysis of small scale micro-grid using renewable energy resources," 2015 International Conference on Electrical Engineering and Information Technology (ICEEICT), pp. 1-4, 2015.

[6] Arsham Iqbal, Ibrahim F. Muhammad, Muhammad Faraz, Muhammad S. Tariq and Hasan-ul Banna, "Economic analysis of a small hybrid power system," 2015 Power Generation System and Renewable Energy Technologies (PGSRET), pp. 1-5, 2015.

[7] M. M. Atiqur Rahman and Ali T. Al Awami, “Decentralized wind-PV-diesel hybrid power generation,” 2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), pp. 1-5, 2015.

[8] L. K. Gan, J. K. H. Shek and M. A. Mueller, "Modeling and experimentation of grid forming inverters for standalone hybrid wind-battery systems," *2015 International Conference on Renewable Energy Research and Applications (ICRERA)*, Palermo,Italy, pp. 449-454, 2015.

[9] Yang Zhang, H. H. C. Iu, T. Fernando, Fang Yao and K. Emami, "Cooperative Dispatch of BESS and Wind Power Generation Considering Carbon Emission Limitation in Australia," in *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1313-1323, Dec. 2015.

[10] D. Arcos-Aviles, J. Pascual, L. Marroyo, P. Sanchis, F. Guinjoan and M. P. Marietta, "Optimal Fuzzy Logic EMS design for residential grid-connected microgrid with hybrid renewable generation and storage," *Industrial Electronics (ISIE), 2015 IEEE 24th International Symposium on*, Buzios, pp. 742-747, 2015.

[11] Wei Li, Jin Pang, QianNiu and Weijia Zhang, "Application of Improved Support Vector Machine Based on Shuffled Frog Leaping Algorithm in Wind-Photovoltaic Battery Power Forecasting," *Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2015 7th International Conference on*, Hangzhou, pp. 128-131, 2015.