IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 10, October 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Morphing Identification with Wireless Sensor Network

[1]D. Kanimozhi ,[2]K.Ravikumar

[1]Research Scholar, Dept.of.Computer Science,Tamil University,Thanjavur-613 010.

[2]Asst.professor, Dept.of.Computer Science,Tamil university,Thanjavur-613 010.

ABSTRACT

One of the mainly vexing problems in wireless sensor network security is the node Morphing attack. An attack, an adversary breaks into a sensor node, reprograms it, with inserts several copies of the node back into the sensor network. Image morphing is a technique to synthesize a fluid transformation from one image (source image) to another (destination image). The source image can be one or more than one images. There are two parts in the image morphing implementation. The first part is warping and the second part is cross-dissolving. Morphing gives the adversary and simple way to build an army of malicious nodes that can cripple the sensor network. In for the most part of a wireless sensor, application security is an individual of the prime concern. Generally, sensor nodes are not equipped with several tamper-resistant hardware and they are deployed in a hostile environment, so the option of occurring attacks should be greater. In node Morphing attack adversary will capture few nodes since the network, retrieving its credentials with creating a large amount of Morphing by reprogramming the nodes. And these Morphing can have the ability to subvert the complete network. So the detection of node Morphing attacks in a wireless sensor network is, therefore, a fundamental problem.

Keywords- ***Morphing Attack, Encryption key, Extract Image, Hide Image***

I.INTRODUCTION

Morphing can be defined as an animated transformation of one image into another image. Morphing involves image processing techniques like warping and cross dissolving. Cross-dissolving means that one image fades to another image using linear interpolation. This technique is visually poor because the features of both images are not aligned, and that will result in double exposure in misaligned regions. In order to overcome this problem, warping is used to align the two images before cross dissolving. Warping determines the way pixels from one image are correlated with corresponding pixels from the other image. It is needed to map the important pixels, else warping doesn't work. Moving other pixels is obtained by extrapolating the information specified for the control pixels. Knowing cross dissolving is very simple, the real problem of morphing becomes the warping technique. Morphing is actually a cross dissolving applied to warped images. Warping techniques vary in the way the mapping of control pixels is specified and the interpolating technique that is used for other pixels.

EXISTING SYSTEM

A wireless sensor network (WSN) is a remote system comprising of an extensive number of geologically dispersed sensor nodes. Security is not included in this system All sensor nodes sense the difference then collects important information and then sends it to base station or gateway by multi-hop communication. WSNs firstly convert data into radio waves and then amplify it and then radio waves are received at receiving node. In many applications of WSNs routing is based on the routing algorithms developed for mobile ad-hoc networks. WSNs are usually very similar to mobile ad-hoc networks (MANETs). As both are distributed network connected wirelessly, use hop-to-hop routing for communication and are battery powered. These sensor nodes could be effectively conveyed at vital districts easily at a low cost. Sensor nodes collaborate with one another to screen physical or ecological conditions, for example, temperature, sound, picture, vibration, weight, movement or contaminations with the assistance of different sorts of sensors. An attack, an adversary breaks into a sensor node, reprograms it, with inserts several copies of the node back into the sensor network.

ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

DRAWBACKS:

- Security issue
- Time waste
- Attack performed
- Integrity issue

II. PROPOSED SYSTEM

Our implementation specifies,the user will specify its ID, which means client id, secret key will be created, and then include the encrypted number. The image will verify the internally bounded user Id and secret key. The witness image means original image. If the verification is a success, the information collecting to the database. , Image morphing is a technique to synthesize a fluid transformation from one image (source image) to another (destination image).The source image can be one or more than one images. There are two parts in the image morphing implementation. The first part is warping and the second part is cross-dissolving. Morphing gives the adversary and simple way to build an army of malicious nodes that can cripple the sensor network.

A new protocol for the detection of attacks. RED is similar, in principle, to the Randomized Multicast protocol, but with witnesses chosen pseudo-randomly based on a network-wide seed. In exchange for the assumption that we are able to efficiently distribute the seed, RED achieves a large improvement over Min terms of communication and computation.

ADVANTAGE OF PROPOSED SYSTEM

- Secure
- Reliable
- Good communication process
- Speed process
- Integrity
- Confidential

III. DIAGRAM

(a) (b) (c)

Figure 2 The results of removing different basis images.(a) original image,(b) result of removing first basis image (c) result of removing the last basis image.

IV. PROCEDURE

MODULES

- APPLY MORPHING
- ENCRYPTION KEY
- EXTRACT IMAGE
- HIDE IMAGE

APPLY MORPHING

Morphing is a **special effect** in **motion pictures** and **animations** that changes (or morphs) one **image** or shape into another through a seamless transition. Most often it is used to depict one person **turning into another** through technological means or as part of a fantasy or surreal sequence.

ENCRYPTION KEY & DECRYPT

Photo **encryption** and decryption, both, can be done from the same interface. To **encrypt** an **image** file you need to browse to the file in the application and choose an **encryption** password. You can also choose to delete the source file after successful **encryption** and conversion of the **image** file.

IMAGE FEATURE EXTRACTION TECHNIQUES

Feature extraction is one of the most significant fields in artificial intelligence. It consists to extract the most appropriate features of an image and assign it into a label. In image classification, the crucial step is to evaluate the properties of image features and to organize the statistical features into classes.

The security of image data from unauthorized users is important hence image encryption plays an important role in hiding information. This survey paper measure up the different encryption techniques for securing multimedia data with the objective to give a complete review on the various encryption techniques.

HIDE IMAGE

You can access your **hidden file** in two ways. Firstly, simply change the extension to RAR and open the **file** using WinRAR. Secondly, you can just right-click on the **JPG** image and choose Open With and then scroll down to WinRAR. Either way, you'll see your **hidden files** show up that you can then extract out.

Viewing the secret message

To view the hidden message or hidden files, you must have followed the above steps. If the above steps were performed to create the image, follow the steps below to view the data.

Tip: You can use the above secret image as an example image if needed.

1. Save the image to the computer, if you're viewing it online.
2. Open WinRAR by clicking Start, Programs, WinRAR, and then WinRAR.
3. Within WinRAR, click **File**, then **Open archive**. Within the open window make sure your files of type option is all files and not just compressed files.
4. Browse to the location of the image and double-click the image to open it.
5. Once open, it should display the file(s) contained within the image that can be extracted from the image.

V.CONCLUSION

An attack, an adversary breaks into a sensor node, reprograms it, with inserts several copies of the node back into the sensor network. **Image morphing** is a technique to synthesize a fluid transformation from one image (source image) to another (destination image).The source image can be one or more than one images. Morphing gives the adversary and simple way to build an army of malicious nodes that can cripple the sensor network. In for the most part of wireless sensor application security is individual of the prime concern.: Wireless Sensor Networks often deployed in hostile environments, where an attacker can also capture some nodes. Once a node is captured, the attacker can re-program it and start replicating the node **Morphing** is a **special effect** in **motion pictures** and **animations** that changes (or morphs).Most often it is used to depict one person **turning into another** through technological means or as part of a fantasy or surreal sequence. 1) lossless reconstruction of the original images, 2) a low pixel expansion ratio to reduce the storage and transmission costs, 3) a low computation cost. The security analysis including theory analysis and experimental demonstration show has a high level of security to withstand the brute-force attack, differential attacks, and a verification function to detect the fake shares.

VI FUTURE ENHANCEMENT

These techniques of image Morphing, compression, and morphing for security enhancement. It has put forward a new system using Morphing which could be proven a highly secured method for data transactions and login in the near future.The new scheme provides and solves many problems of the existing system. It can also be useful for the user in security point of view. No password information is exchanged or changed between the client and the server. Since the authentication information is conveyed, it can secure of many attacks, which none of the existing schemes can tolerate. The security is enriched and used in online banking in our project. Also the same can be used in any field which requires user authentication. The use of morphing image with morphing can be done on furthermore sectors.

REFERENCE

1. F Arab, S Paneels et al., "Haptic patterns and older adults: To repeat or not to repeat?", *IEEE WorldHaptics*, pp. 248-253, 2015.

2. D. Sheela, Srividhya. V. R, Vrushali, Amrithavarshini and Jayashubha J. "A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks", ICCTAI'2012.

3. Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks", IEEE Transactions On Dependable And Secure Computing, VOL. 8, NO. 5, 2011.

4. LM Brown, Y Kaaresoja, "Feel Who's Talking: Using Tactons for Mobile Phone Alerts", *CHI '06 Ext Abs CHI '06*, pp. 604, 2006.

5. Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei, "Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN", IEEE International Conference on Systems, Man and Cybernetics, 2006, Taiwan.