Software Piracy Detection and Prevention Using Sift Algorithm with Two-Way Authentication Mechanism

Soyemi, Jumode & Adesi, Adesola
Department of Computer Science
he Federal Polytechnic
Ilaro, Ogun State, Nigeria
E-mails: jumoke.soyemi@federalpolyilaro.edu.ng; adesiadesolabolaji@gmail.com
Phones: +2348052848284, +2347069005739

ABSTRACT

Software industry contributes to the world's economy growth and development by advancing society through technological innovations. Software is an intellectual property and piracy of software which is an unlawful duplication of copyrighted computer software has been a major setback in software industry over the years and this has hampered the revenue generated with the high cost of investment in developing such software. Despite, the diversity of technical measures against illegal duplicating of software, most existing protection methods failed in protecting software. This study proposed image splitting system with two-way authentication techniques to validate security details before installation can begin on host computer. This activation algorithm uses image of the activator that is split into half and secured on different servers compared with the current image of the activator captured to generate an authentication key that will be required during installation and activation of the software. In addition, the host machine details will be extracted and tied to the image generated. The proposed system guarantees better security.

Keywords: Software piracy, Sift Algorithm, Two-way Authentication mechanism, Key Generation, Facial Authentication

iSTEAMS Proceedings Reference Format
Soyemi, J & Adesi, A. (2019): Software Piracy Detection and Prevention Using Sift Algorithm with Two-Way Authentication Mechanism. Proceedings of the 16th iSTEAMS Multidisciplinary Research Nexus Conference, The Federal Polytechnic, Ilaro, Ogun State, Nigeria, 9th – 11th June, 2019. Pp 59-66-. www.isteams.net - DOI Affix - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V16N1P8

1. INTRODUCTION

Software use spreads across several sectors of the society both large and small organizations including individual personal use to carry out important tasks. However, software is being pirated on a large scale (Srinivas, Venkata and Varma, 2012) making the developers to be at the receiving end. Software piracy is an unlawful duplication of copyrighted computer software (Shen, 2005) without authorization from the developer. This theft of intellectual property is now one of the biggest and visible challenges in computing today (Peace, Galletta and Thong, 2003) and a big economic concern to several software organizations (Pawar, *et al*., 2016). The increase in the number of computer software piracy is because computer software is easy to reproduce, relatively easy to copy and does not result in a ruin on the quality of the product. Also, because of the high number of personal computers that are available. Companies operating in the field of software business regularly face harms caused by software piracy, one of which is the loss of revenue. Most of the software activations are done at the user end, such as key validation and integration of hardware which makes it so easy for anyone to get hold of executable software and carry out tapping activity. Software cracking is achieved after much time and efforts by the pirates (Srinivas, Venkata and Varma, 2012).

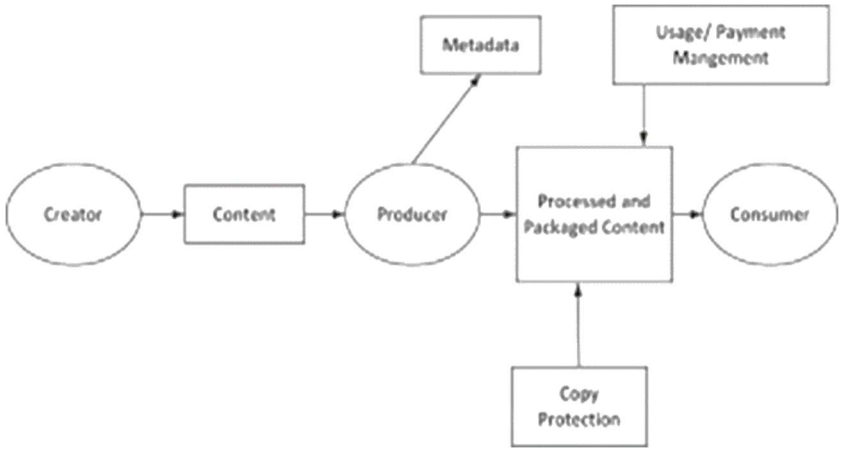

Fig. 1: Software Detection and Protection Framework
Source: Sciencedirect

Some of the several ways in which software are being pirated includes; cracks and serials which is quite very common, and is implemented by either entering a certified code or engaging a patch that disengages the copyright protection (Anckaert, Sutter and Bosschere, 2004). Soft lifting is another means in which software is obtained with the consent to be installed on specific number of systems but are installed on more than the allowed system. Hard lifting on the other hand deals with unlawful installation of software on hardware (Anckaert, Sutter and Bosschere, 2004). Another means of software piracy is Internet piracy and software counterfeiting. While internet piracy is an unlawful copying of copyrighted software through electronic means especially, the internet, software counterfeiting is an unlawful duplication and distribution of copyrighted software (Goertzel, 2011). Mischanneling is another means that uses academic license for commercial purposes.

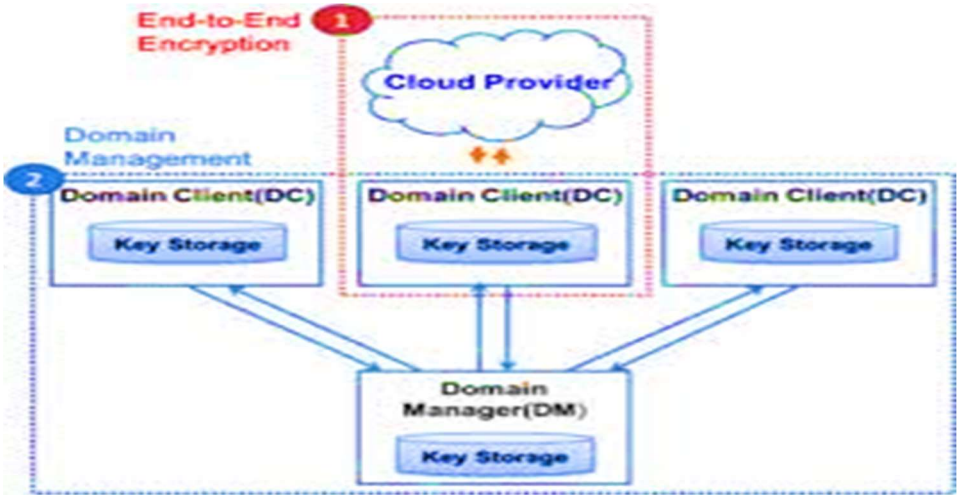

Fig 2: Protection Mechanism Framework
Source: Sciencedirect

Although, there are quite a number of anti-piracy methods available for use in the market such as license key, activation code, file and others to protect software asset but there continue to be the constant rise in software piracy, this however has been associated with those methods being too expensive to implement or too easy to be defeated or not convenient to use (Chandu, Singh and Baskaran, 2008). There are also several research methods carried out on software piracy detection and prevention, most especially on the technical aspect, but such methods have not been able to prevent piracy.

There are basically two methods against software piracy which can either be preventive and deterrents. While deterrent methods target hindering users from pirating software by enforcing legal penalty, the preventive methods make pirating so difficult that the perpetrators deplete their resources and are forced to withdraw. (Laith, 2017; Gopal and Sanders, 1997).

This research work proposed the deployment of SIFT algorithm to extract regions of interest of image submitted by a user at a point and compare this to later image submitted. The extracted features are invariant to scaling and distortion with strong matching ability.

2. RELATED STUDIES

Image matching techniques with local features of interests' dates back to the research of Moravec (1981) where he used a corner detector on a stereo matching. The research work of corner detector laid the needed foundation for Harris and Stephen (1988) to work extensively on image variations and near edges detection to capture image locations with large amounts of gradients from different angles at a predetermined scale. Zhang *et al*. (1995) posited that correlation window will be necessary around the corner to select likely regions. The research work of Schmid and Mohr (1997) introduced invariant local feature techniques, where matching of images can be done across large dataset.

These features allowed comparism between two images with changes in orientation to one of the images. Lowe (2004) designed an algorithm called Scale Invariant Feature Transform, SIFT and this algorithm works by extracting the distinctive invariant features from images presented and later compare it with new image supplied to match the area even with different position of the object. SIFT transform image supply to the system into coordinates of x, y of the pixels and store such image into the database, the process of computation occur if a new image is supplied to the system, such image features are also extracted and relate those coordinates to the object already stored for image matching and recognition despite their orientation.

This research work proposed image splitting algorithm with two-way authentication techniques to validate security details before installation can begin on host computer. This activation algorithm uses image of the activator that is split into half and secured on different servers compared with the current image of the activator captured to generate an authentication key that will be required during installation and activation of the software. In addition, the host machine details will be extracted and tied to the image generated.

3. METHODOLOGY

Scale Invariant Feature Transform (SIFT)

SIFT features are features extracted from images to help in reliable matching between different views of the same object. The extracted features are invariant to scale, and orientation are highly unique of the image. Here, features are extracted for user submitted images, because using SIFT approach enables easily comparison of images despite their orientation in different directions. These generated features are used for image comparison and the generation of unique key for validation.

Feature extraction

Feature extraction for this algorithm is achieved by getting a set of unique properties or local properties extracted from every image. Such properties include; position, Scale, orientation and detailing of the image's local structure.

Preprocessing

Preprocessing of the image extracted is performed to enhance the target image in order to get better result. The preprocessing operation required here are to convert input image into HSV form from RBG, then perform thresholding and summation which is applied to combine the two images from the thresholding step to produce one image. Finally, gaussian blurring which is the last step of preprocessing is done to make the image smooth and remove the noise and unwanted details.

The Proposed System

The proposed system requires a centralized activation server that is competent enough to make secured validations using image matching and features extraction based on Earth movers distance algorithm and SIFT algorithms (Figure 1 and Figure 2). Figure 1 represents the Architecture of the system and Figure 2, the pipeline of the proposed system. This study combines an activation tool along with software distribution which will be used to carry out validations and activation at users end.

The point of call is for user to submit an image through the webcam at the point of registration through an account, features are extracted from this image using SIFT approach and stored in the database. At some stage in software activation using integrated tool, user submits the same image which he had submitted during software purchase, or takes a photo using system webcam. This image is sent to activation server and the features of the new image is extracted and compared to the features of the image in the server, if the features matches, the algorithm generates an activation key for the user which he uses in completing software installation process.

The SIFT algorithm selects the key point areas which is the region of interest of the first image submitted and stored those features in database. The regions are calculated through the difference of the Gaussian interpolation. The extracted features are invariant to scaling and distortion with strong matching ability. Both figures 1 and 2 show the process of authenticating the first stage of the process through image analysis and matching of regions on which led to the second stage where a generated pass key is displayed. The MAC address of the host machine in which the software is being installed, captured and tied to the image so that no other user can use different image on that machine.

A large key with varying sizes is generated using image features and software ID, some system properties are also added to the key at the client side to make it unique and this key contains or represents software validation and authentication. Even though, a hacker or cracker tries to bypass this activation process, this key file should be present to run software, this key file adds more advantage so that software usage can also be tracked and if any misuse of software or piracy attempts can be recorded and reported. This key file is distributed from activation server to activation setup system at client end. A three-step process is undergone by client and server to exchange this key file. After authentication at server, it sends a key ready signal to client and client respond with a key request by encapsulating system properties. Now server generates a unique number using system properties and encrypts key file contents with that unique number and transfers it to client. Upon receiving key file, client decrypts it and loads key into secure place and adds a reference to software executable and generates a loader executable. This executable is launched to execute the original software.

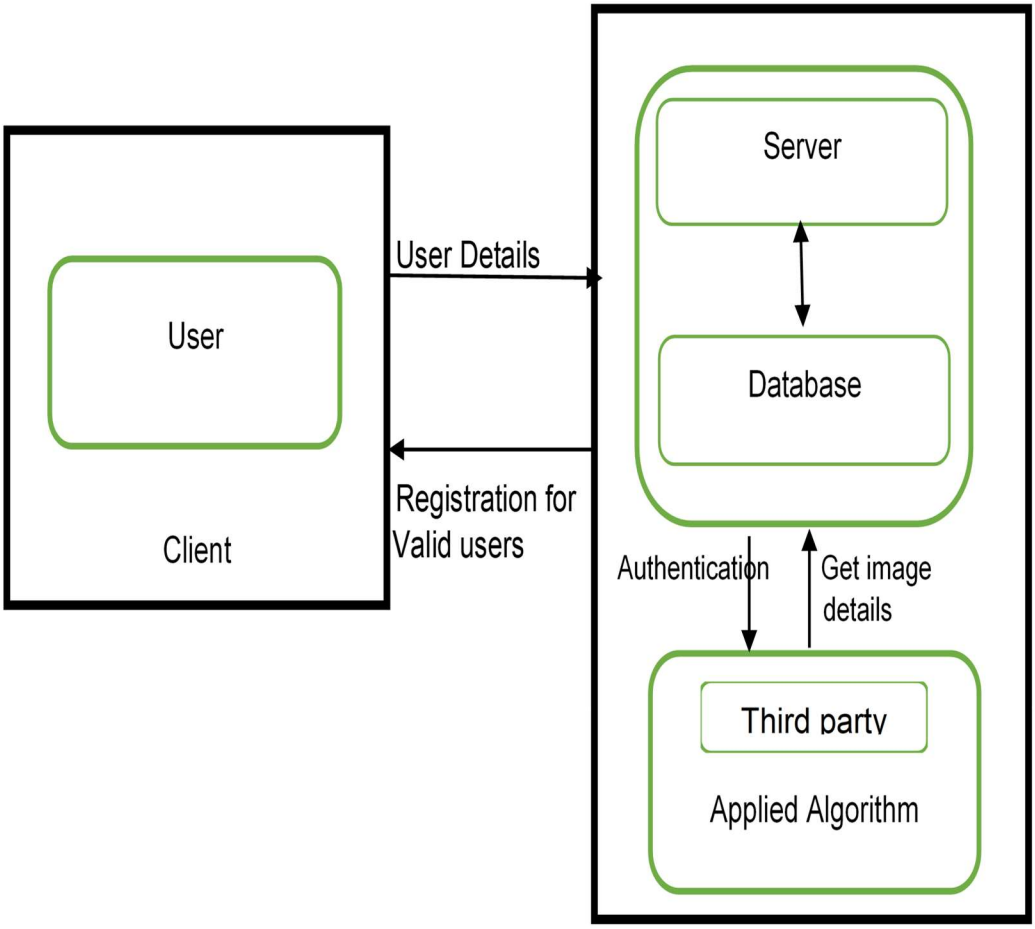

Figure 1: Architecture of the System

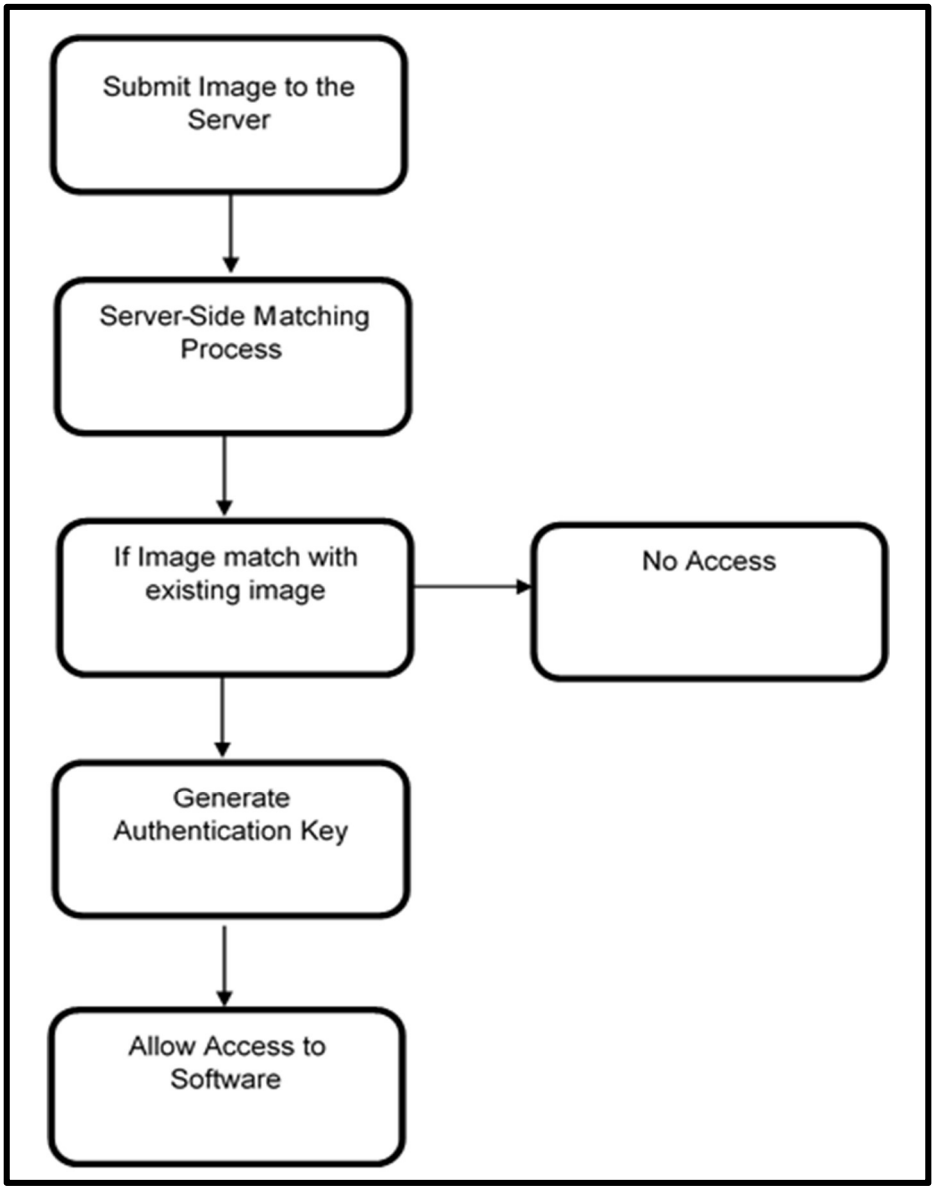

Figure 2: Pipeline of the Proposed System

4. CONCLUSION

The proposed system for software piracy detection and prevention here, made use of images rather than keys, and the images are split for security purposes. Splits images does not have extension and retrieving them are not possible. Aside from this, it is impossible to generate the exact replica of the image because only the server has the original image. Thus, making hacking or cracking of software using traditional methods very difficult to achieve. Therefore, this proposed system when implemented and deployed, guarantees zero tolerance to software piracy.

REFERENCES

1. Anckaert, B., De Sutter, B., and De Bosschere, K. (2004). Software piracy prevention through diversity In Proceedings of the 4th ACM workshop on Digital rights management.
2. Chandu, V.P., Singh, K. and Baskaran, R. (2008). A model for prevention of software piracy through secure distribution. Advances in Computer and Information Sciences and Engineering, 251-255.
3. Gbash, E.K. and Saleh, S.M. (2017). Scale-Invariant feature transform Algorithm with fast approximate Nearest Neighbour. Baghdad Science Journal, 14(3):651-661.
4. Goertzel, K. M. (2011). Protecting Software Intellectual Property against Counterfeiting and Piracy.
5. Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. Journal of Management Information Systems, 13(4), 29-47
6. Harris, C. G. and Stephens, M. (1988). A combined corner and edge detector. In Alvey vision Conference 15(50): 10-5244.
7. Laith, T.R. (2017). Software piracy solutions. International Journal of Computer Science and Mobile Computing, 6(2):156-169.
8. Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. International journal of computer vision, 60(2), 91-110.
9. Moravec, H. (1981). Rover visual obstacle avoidance. International Joint Conference on Artificial Intelligence, Vancouver, Canada, pp. 785-790.
10. Pawar, C., Badekar, A., Petkar, K., Chaferkar, A., Baber, N. and Kadam, V. (2016). Software piracy prevention. International Research Journal of Engineering and Technology, 3(3):1642-1643
11. Peace, Dennis and Thong (2003). Software piracy in the workplace: A model and empirical test. Journal of Management Information Systems, 20(1):153-177.
12. Shen, X. (2005). Developing Country Perspectives Software: Intellectual Property and Open source International Journal of IT Standards and Standardization Research (IJITSR), 3(1), 21-43.
13. Schmid, C., and Mohr, R. (1997). Local grayvalue invariants for image retrieval. IEEE Trans. on Pattern Analysis and Machine Intelligence, 19(5):530-534.
14. Srinivas, B., Venkata, K. and Varma, P.S. (2012). Piracy detection and prevention using SIFT based on Earth Mover's Distance (EMD). International Journal of Computer Applications, 38(7): 35-41.
15. Zhang, Z., Deriche, R., Faugeras, O., and Luong, Q.T. (1995). A robust technique for matching two uncalibrated images through the recovery of the unknown epipolar geometry, Artificial Intelligence,78(28): 87-119.