IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Simulation Based Exploration of SKC Block Cipher Algorithm

T. Sai Iswarya[1*], K.Rangaswamy[2]

[1] Department of Computer Science, Alts, anantapur
[2] Department of Science and Technology, Alts, anantapur

Corresponding Author: aish.tippaluru@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i6.11491152 | Available online at: www.ijcseonline.org

Accepted: 24/Jun/2019, Published: 30/Jun/2019

***Abstract*—** Social media provides an environment of information exchange. They principally rely on their users to create content, to annotate others' content and to make on-line relationships. The user activities reflect his opinions, interests, etc. in this environment. We focus on analyzing this social environment to detect user interests which are the key elements for improving adaptation. This choice is motivated by the lack of information in the user profile and the inefficiency of the information issued from methods that analyze the classic user behavior (e.g. navigation, time spent on web page, etc.). So, having to cope with an incomplete user profile, the user social network can be an important data source to detect user interests. The originality of our approach is based on the proposal of a new technique of interests' detection by analyzing the accuracy of the tagging behavior of a user in order to figure out the tags which really reflect the content of the resources. So, these tags are somehow comprehensible and can avoid tags "ambiguity" usually associated to these social annotations. The approach combines the tag, user and resource in a way that guarantees a relevant interests detection. The proposed approach has been tested and evaluated in the Delicious social database. For the evaluation, we compare the result issued from our approach using the tagging behavior of the neighbors (the egocentric network and the communities) with the information yet known for the user (his profile). A comparative evaluation with the classical tag-based method of interests detection shows that the proposed approach is better

***Keywords*—**MCP, Feedback, Relavance

I. INTRODUCTION

The Web is changing at a very fast pace, whether it be the content versatility or it be the technology that explores the web content in meaningful and useful information. Figure 2-1 shows the pyramid of the Web evolution (Spivack, 2007). The divisions on the pyramid represent the volume of information in each version of the Web. The right side shows the technologies that have been used, are being used or expected to be used in the future as shown as per the evolution time period shown on the left side of the pyramid. The World Wide Web (Web 1.0) which is primarily based on hyperlinks requires keywords, co-occurrence and page rank for searching relevant web pages. The relevance of web pages in this face of the Web is usually computed using hubs and authorities (Kleinberg & Lawrence, 2001) or, keyword term frequency (Salton & Buckley, 1987). However, these techniques and other traditional search algorithms besides being simple and computationally sound, lack in searching semantically relevant web pages (Navigli & Velardi, 2003). This means that the pages that contain synonyms, hypernyms or hyponyms for the keywords rarely get incorporated during the search. The World Wide Web (WWW) being the first version of the Web is usually referred as '**Web**' in early literature. However, in the thesis the Web has been used for the existing Web consisting of the WWW, the Social Web and the Semantic Web. To refer a specific version of the Web, these will be referred in particular. As mentioned earlier, the WWW is a vast collection of web pages interconnected with each other through web links called hyperlinks. *Web page*, a unit of information on the WWW has many synonyms like *document*, *resource* and *page* (Sebesta, 2007). These synonyms have been used interchangeably depending on the context in the thesis. Information retrieval has attained new definitions with the advent of the Web. The web information retrieval deals with the representation, storage, organization of, and access to information items (Baeza-Yates & Ribeiro-Neto, 1999). Low cost, greater access, publishing freedom and linking documents to many other documents on the Web are the primary reasons for the popularity of the Web as a highly interactive medium and immeasurable source of information. Searching useful information to users' interest in the ever-growing volume of the Web is a real challenge for Web information retrieval research.

In a conventional information retrieval system a document is described logically as a collection of index terms. An index term is a keyword which has some meaning of its own such as nouns. In general, the index term may consist of all words in text of the document. However, considering index in this way raises concerns over the text semantics. This issue has been discussed many times in the information retrieval literature. These index terms are compared to find similarity or relevance of the document to a query using various models. The **web retrieval process** can be explored in one of the two operational modes, ad-hoc and filtering. In **ad-hoc retrieval**, the documents in the collection remain relatively static while new queries are submitted to the system. In the other mode, the queries relatively remain static while new documents come in the system (and/or leave the system). This operational mode is termed as filtering. The work in the thesis belongs to the filtering task. In **filtering**, the ranking of documents is based on the users' information need, which is usually constructed through a set of keywords provided either by a user explicitly or extracted implicitly through some preferred relevant documents. This initial information need to improve searching is sometimes referred as 'user profile' or expansion of the query/topic which takes care of a user's information needs. The simplistic way to construct the expanded topic list is to ask user to provide keywords related to his/her search requirement. In some cases the user is also asked to provide relevance feedback about the searched documents to build a training set (consisting of two sets of relevant and non-relevant documents) to be used for improving future retrieval results. Though this approach is simple, it requires a user to provide lot of details that describes his/her profile. Moreover, the user is expected to be familiar with the search topic. (S)he has to provide related keywords or required to be able to judge the relevance of documents. The work in the thesis has adopted an approach to construct an expanded topic list for filtering by using semantic knowledge on a search topic. Constructing expanded topic list using semantic structure (consisting of the search topic and its useful related concepts) has a number of benefits towards the filtering task as compared to the above mentioned method. The semantic structure based topic expansion methods alleviates the need for the user to provide related keywords on the required search topic and neither the user is required to spend time in constructing the training set. Context sensitive document retrieval is the added benefit of the semantic structure based filtering.

II. RELATED WORK

Feature selection (FS) is a search process in the field of data mining which selects a subset of salient features to build learning paradigm such as decision trees and neural networks. Some irrelevant and/or redundant features usually exist in the training data which makes learning tougher and also degrades the performance of trained model. More precisely, good FS techniques can detect and ignore noisy and false features. This process leads to increasing the quality of dataset after feature selection. Two quality factors need to be considered here: relevancy and redundancy. A feature is said to be relevant if it is prognostic of the decision feature(s); else it is irrelevant. A feature is deemed to be redundant if it's correlation with other features is high. An informative feature must be highly correlated with the decision concept(s), but it is highly uncorrelated with others. Many feature selection algorithms are involved in heuristic or random search methods in order to decrease the time complexity.

In [1] Anelia Grigorova, Francesco G. B. De Natale, Charlie Dagli, Thomas S. Huang, Life Fellow, presents a feature adaptation techniques to retrieve more relevant images. It is an effective feature space dimension reduction according to user's feedback, but also improves the image description during the retrieval process by introducing new significant features. FA-RF uses two iterative techniques to make use of the relevance information that is query refinement and feature re-weighting. For the adaptation of across RF uses the descriptions of both relevant and irrelevant image, as well as their number and proportions. The query image is located near to the boundary of the relevant cluster in the feature space then the system contains few relevant images. Thus the query refinement mechanism is useful to move the query towards the middle of the cluster of relevant images in the feature space. This FA-RF performs very well in terms of capability in identifying most important features and assigning them higher weights compared with classical feature selection algorithms. Also maintain compact image description. The main drawbacks are less efficient for large databases. There is also needs an efficient feature extraction algorithm. In [2] Mohammed Lamine Kherfi and Djemel Ziou proposed a new RF framework that combines the advantages of using both the positive example (PE) and the negative example (NE). This method learns image features and then applies the results to define similarity measures that correspond to the user judgment. The use of the NE allows images undesired by the user to be discarded, thereby improving retrieval accuracy. This method tries to learn the weights the user assigns to image features and then to apply the results obtained for retrieval purposes. It also reduces retrieval time. It clusters the query data into classes and model missing data, and support queries with multiple PE and/or NE classes. The main function of this method is that it assigns more importance to features with a high likelihood and those which distinguish well between PE classes and NE classes. The drawbacks are small sample problem. Also the use of PE is sufficient to obtain satisfactory results. In [3] Dacheng Tao, Xiaoou Tang, Xuelong Li and Xindong Wu, presents an Asymmetric Bagging and Random Subspace based Support Vector Machine (ABRS-SVM) to solve the problems of SVM in image retrieval and over fitting

problem. In [4] Ja-Hwung Su, Wei Jyun Huang, Philip S. Yu, Fellow, and Vincent S. Tseng, proposed a Navigation Pattern based Relevance Feedback (NPRF) achieve high efficiency and effectiveness with the large scale image data. Also reduces number of iterative feedbacks to produce refined search results. The iterative feedbacks are reduced substantially by using the navigation patterns discovered from the user query log. This NPRF approach is divided into two operations that is the online image retrieval and offline knowledge discovery. NPRF Search makes use of the discovered navigation patterns and three kinds of query refinement strategies such as Query Point Movement (QPM), Query Reweighting (QR), and Query Expansion (QEX). The query image is submitted to this system, and then the system first finds the most relevant images and returns it. This process is called initial feedback. Next, the positive samples picked up by the user is given to the image search phase including new feature weights, new query points and user's intention. Navigation patterns with three search strategies are included to find the desired images. For each user's browsing behaviors, offline operation for knowledge discovery is triggered to perform navigation pattern mining. The main drawbacks of this system are image retrieval in global feature space and results depends only on the navigation pattern of users. In [5] Wei Bian and Dacheng Tao proposed a new dimensionality reduction algorithm for relevance feedback in the content based image retrieval is called Biased Discriminative Euclidean Embedding (BDEE). The samples in the original dimensional ambient space is transformed to low level visual features to discover intrinsic coordinates of an image. BDEE models both the interclass geometry and interclass discrimination of each image. It does not ignore the manifold structure of samples. BDEE is a subspace learning method in which mapping vector is used to map high dimensional space to low dimensional space. In [6] Yu-Chen Wang, Chin Chuan Han, Chen-Ta Hsieh, YingNong Chen, and Kuo-Chin Fan proposed a Feature Line Embedding Biased Discriminant Analysis (FLE-BDA) for performance enhancement in relevance feedback scheme. It maximizing margin between relevant and irrelevant samples at local neighborhood so that relevant images and query image can be quite close, while irrelevant samples are far away from relevant samples. In this subspace learning method, find a linear transformation matrix from relevant or irrelevant images that is used in dimensionality reduction. The retrieval process includes 1) A query image is inputted to the IR system. After calculating the similarity values, gallery images are ranked. 2) Users label the relevant or irrelevant images according to their preference. 3) Then user's' feedback is adopted to find a new transformation. 4) The gallery images are re-ranked to obtain the retrieval results in the next round. Two labels are assigned to the top ranking images according to users' preference. Feedback with relevant or irrelevant labels represents users' preference. The within class scatter is calculated from the image samples with positive labels, while the between-class scatter is calculated from those with negative labels. Based on these assigned labels, the within class and between-class weighted graphs are constructed for maximizing the margin of relevant and irrelevant samples. Then new distance between query and images are calculated. The advantages are dimensionality reduction, solve singular problem in the high dimensional space, increases generalization and robustness using Laplacian regularization. The disadvantage are computational complexity is very high due to the large scale dataset. In [7] Lining Zhang, Lipo Wang, and Weisi Lin [3] proposed an conjunctive patches subspace learning (CPSL) method for learning an effective semantic subspace by exploiting the user historical feedback log data with the current data. CPSL effectively integrate the discriminative information of labeled log images, geometry information of labeled log images and weakly similar information of unlabeled images. For creating a reliable subspace, need to build different kinds of local patches for each image. Apart from other Relevance Feedback techniques, Collaborative Image Retrieval system integrates regular online RF schemes with an offline feedback log data. From the figure, the CIR systems first collect RF information from user which can be stored in an RF log database. If user feedback log data is unavailable then the CIR system performs exactly like RF based CBIR system. If the user RF information is available, the algorithm can effectively exploit the user feedback log data. The image retrieval can be done in less iteration than regular RF schemes with the help of the user historical feedback log data.

III. METHODOLOGY

We present the general algorithm of our approach in Table 1 and then the detail of each function. This algorithm is applied for all users U. The function Add(param1, param2), allows us to add the param2 into the param1. So, there no overwriting of the param1.

We begin with generating the relevant resources R' to a given tag, where $R' = \{r'_1, \ldots, r'_v\}$ the set of relevant resources and v the number of relevant resources and $R' \subseteq R$. We use the function Add() in order to add each relevant resource into R'. This step interrogates the Index File (the output of the indexation step). When a request/query is made it is treated by the same analyser used to build the index and then used to find the corresponding term(s) in the index. This provides a list of resources matching the query. In our context, a query is considered as a tag throughout the rest of this paper. We present the algorithm of generation resources relevant to a given tag $t_h \in T$ (see Table 2).

After generating relevant resources (R') according to a specific tag (t_h), a score is assigned to each resource according to the assigned tag. The purpose of using such

score is to separate the most relevant resources related to a specific tag. This score is the result of a function of similarity which takes into consideration the resource (textual) and the tag. Many similarity functions exist in the literature such as the similarity function supported by Lucene. We choose a predefined function[6] of similarity which is a variant of the TF-IDF scoring model. The choice of such a model is due to the fact that TF-IDF is an efficient and simple algorithm for matching words in a tag to resources that are relevant to that tag. However, the main limitation of such a model is that it does not take into consideration the relations between words (e.g. synonyms). The similarity function is described through the formula (1) as follows:

The term t is the result of the resource indexation process. Each term t is associated with a resource r.
After scoring the resources, we test if the resource tagged by q exists in the top-k result provided by the scoring function. If it is the case, the tag q is stated as relevant to the resource.

IV. RESULTS AND DISCUSSION

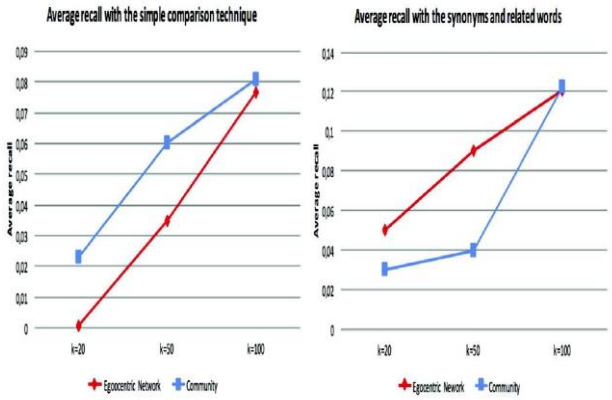

Fig1: Average recall

V. CONCLUSION AND FUTURE SCOPE

In this paper, we have proposed an approach for detecting accurate user interests based on the social environment. The goal was to infer users interests from content of the tagged resources in order to figure out the tags really reflecting the thematic of the resources. The originality of our approach is based on the proposal of a new technique of interests detection by analysing the accuracy of the tagging behaviour of a user in order to figure out the tags which really reflect the content of the resources. So, these tags are somehow comprehensible and can avoid tags "ambiguity" usually associated to these social annotations. This is done through an indexation technique followed by an algorithm that score tags assigned to resources. This score reflects the relevance of the tag according to a resource. From this score, we have selected the most relevant resources (top-k). If the tag assigned by the user to a resource that is in the top-k, then the tag is considered an accurate interest. The experiment shows that our method provides a comprehensible set of interests. Consequently, our approach could be used for a purpose of adaptation (e.g. enrichment of the user profile, recommendation, etc.), since it provides a solution for detecting relevant user interests. The results have proved that the consideration of the tagged resources to detect the relevant user interests (our approach) is better than considering directly the tags assigned by the users (classical tag-based approach). In fact, our approach has treated the tag ambiguity and then, has provided better results..

REFERENCES

[1] P. L. Stanchev and D. G. Jr, "Current state and research trend in the image database systems," mathematics and education in Mathematics, Brovoez, pp. 66–76, 2002.
[2] D. F. Long, D. H. Zhang, and P. D. D. Feng, "Fundamental of content based image retrieval," research Microsoft, 2003.
[3] S. Jain and S.N.Pradhan, "Enhancement of color image retrieval capabilities: function of color with texture(optimized)," NUCON 2007,Nirma University, December 2007.
[4] I. Valova and B. Rache, "Retrieval by color features in image databases," International Conference on Computer Systems and Technologies - CompSysTech2002, 2002.
[5] I. Valova and B. Rachev, "Image databases an approach for image segmentation and color reduction analysis and synthesis," International Conference on Computer Systems and Technologies - CompSysTech2003, 2003.
[6] I. Valova, B. Rachev, and M. Vassilakopoulos, "Optimization of the algorithm for image retrieval by color features," International Conference on Computer Systems and Technologies - CompSysTech, 2006.
[7] R. M. Hralick, "Statistical and structural approaches to texture," IEEE .67, p. 786805, 1979.
[8] M. Amadasun and R. King, "Texural features corresponding to texural properties," IEEE Transaction on system, Man and Cybernatics, 1989.
[9] S. C. Hoi, M. R. Lyu, and R. Jin, "A unified log-based relevance feedback scheme for image retrieval," IEEE Transaction on knowledge and data engineering, Vol. 18, No. 4,, April 2006.
[10] Tesic.J. and M. B, "Nearest neighbour search for relevance feedback. in computer vision and pattern recognition," IEEE Computer Society Conference, Volume 2,pp. 18–20, June 2003.

