

ABSTRACT

The present application discloses a biometric matching method, terminal device, server, system, and medium, and belongs to the field of data processing. The method includes: performing, based on a first private key, an acquired biometric vector to be matched, a preset generating element, a second private key, and first encrypted data, a number of interactions and processes with a server to obtain second encrypted data (S201), the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator including the second private key and a target Euclidean distance being formed in the second encrypted data; and sending the second encrypted data to the server to cause the server to obtain, using the second encrypted data, the generating element, the second private key, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector (S202).

Fig. 2